4. НЕТРАННИНГ

Перевод (c) Sergeant
Правка (c) Junior

Сердечная благодарность Unseen'у и всем посетителям сайта http://www.rpg.kiev.ua за помощь в переводе

Идея всемирной сети, а также идеи контроля за доступной в сети информацией, ее изменения или похищения является общей темой киберпанк литературы. Иногда, как в "Сожжении Хром" Уильяма Гибсона, все действие разворачивается вокруг компьютерной кражи. В других случаях сеть лишь мимоходом участвует в сюжете, являясь, однако, важной частью окружающего мира.
Мастер может придерживаться различных взглядов на роль компьютеров в мире киберпанка. Некоторые из них, от реалистичных и правдоподобных до псевдонаучных и мистических, излагаются в этой главе.

ЧТО ТАКОЕ СЕТЬ?

Множество компьютеров оборудовано устройствами, которые позволяют им соединяться с другими компьютерами - модемами, пакетными контроллерами, волоконно-оптическими интерфейсами, спутниковой связью и т.п. Эти компьютеры соединяются с другими компьютерами, которые, в свою очередь, соединяются с другими компьютерами, образуя огромную разветвленную сеть.
Каждая машина в сети называется "узлом". Типы компьютеров, подключенных к сети, варьируются от простейших терминалов ввода-вывода (которые предоставляют доступ к сети, но не способны обрабатывать данные) и небольших персональных компьютеров или кибердек (они чаще всего используются персонажами) до университетских вычислительных машин и банковских мейнфреймов или огромных корпоративных искусственных интеллектов (ИИ).
Если мастер планирует позволить своим игрокам исследовать сеть, он должен сначала нарисовать ее "карту", решив, какие компьютеры подключены к сети, какими путями должны пойти персонажи и какие меры безопасности принять, чтобы добраться до них. В главе "Отображение Сети" на стр. 82, вы найдете советы и таблицы для создания участков сети случайным образом.
Кроме того, мастеру следует решить, насколько "реалистичен" его мир - предпочитает ли он использовать существующую вычислительную технику или погрузиться в сияние *киберпространства*.

РЕАЛИСТИЧНЫЕ СЕТИ

Многих мастеров и игроков не заинтересуют киношные изгибы киберпространства - их кампании будут или проходить в недалеком будущем, так что необходимые нейро-интерфейсы (см. стр. 72) технологически еще недостижимы, или мастер попросту захочет создать свою сеть путем использования существующих образцов техники. Это абсолютно нормально - помните, что в жанре киберпанка главное борьба, а не компьютеры!
В "реалистичной" кампании не будет нейро-интерфейсов и кибердек - только обычные компьютеры, очень похожие на существующие сейчас.
Читатели, интересующиеся киберпространственной моделью компьютерной сети, должны сначала прочитать этот раздел, поскольку в правилах по киберпространству будут ссылки на многие из затронутых здесь вещей.

Компьютеры

Компьютеры впервые появились в раннем TL6. К TL7 они уже становятся жизненно важными для общества, а на более высоких технических уровнях их роль продолжает возрастать. Нижеследующие правила могут использоваться для компьютеров любого TL, но упор будет сделан на компьютеры ближайшего будущего, предназначенные для "реалистичного" киберпанка.
Любой компьютер может быть подключен через устройство связи или сетевой кабель к другому компьютеру. После этого меньший компьютер становится терминалом большего, позволяя (по крайней мере теоретически) использовать все его возможности. Конечно, чтобы войти в систему, пользователь должен знать - или найти - необходимые пароли. По-другому получить доступ к защищенному компьютеру очень трудно; см. "Компьютерная безопасность" на стр. 69.

Аппаратные средства

Компьютеры классифицируются по степени Сложности (Complexity) - это характеристика не самого компьютера, а тех программ, которые он способен выполнить. Простейшие компьютеры обладают Сложностью 1; компьютеры Сложности 6 и более могут обладать самосознанием.
Каждый уровень Сложности означает производительность в 10 раз большую, чем раньше. Компьютер Сложности 3, например, в 10 раз быстрее, чем компьютер Сложности 2 и в 100 раз быстрее, чем компьютер Сложности 1. Подробнее см. "Программное обеспечение", стр. 64.

Типы компьютеров

Специализированный компьютер: Само устройство данной системы подчиняет все ее мощности выполнению одной задачи. Компьютер выполняет одну-единственную встроенную в него программу, которую нельзя заменить. Сложность компьютера равна Сложности программы. Его стоимость обычно на (1d x 10 %) меньше, чем стоимость такого же универсального компьютера, плюс стоимость самой программы.
Персональный компьютер: В кампании, которая не использует киберпространство (стр. 72), большинство персональных компьютеров будут обладать Сложностью 2, хотя высококлассное оборудование, разработанное для правительственных или корпоративных агентов, может иметь Сложность 3 (или даже 4!).

Обычный персональный компьютер будет снабжен цветным монитором с высоким разрешением (некоторые - с сенсорной чувствительностью), клавиатурой, мышью или трекболом, и каким-либо голосовым интерфейсом. У него будут разъемы для подключения устройств типа принтеров или плоттеров, и порт, через который по линии связи можно будет получить доступ к сети.
Он легко помещается в портфель, весит 2 фунта, стоит 1,000 $ и работает год на B-батарее.
Миникомпьютер: Это - рабочая лошадка компьютерного бизнеса. При TL8 почти каждый дом среднего класса будет наделен таким "домашним мозгом". В мелком бизнесе или в отдельных подразделениях большего также будут использовать такие мини-системы. При TL8 миникомп обладает Сложностью 3 и стоит 15,000 $. Он может работать от сети на 110 или 220 вольт, или шесть месяцев на C-батарее.
При TL8 самый маленький мини-компьютер весит 30 фунтов. Его размеры и форма определяются назначением, но обычно это плоский корпус размерами около 2 x 12 x 20 дюймов с откидываемым экраном и выдвижной клавиатурой. У этой модели обычно есть ручка и крепления для ремешков, так что ее можно носить как ранец. Высокая стоимость (30,000 $) обусловлена мобильностью этой системы.
Микрофрейм: Многопользовательская система Сложности 4 предназначена для использования на больших пассажирских судах или в университетских центрах. Базовая стоимость системы - 40,000 $, плюс 2,000 $ за каждого пользователя. Микрофрейм весит около 400 фунтов и занимает примерно 4 кубических ярда; он работает от сети или шесть месяцев от E-батареи.
Мейнфрейм: Используется для управления и наблюдения за работой крупного предприятия, производственного комплекса или лаборатории. Он обычно подключается к основному источнику питания судна или здания и может иметь резервное питание - комплекс из 50 E-батарей (которые обеспечат его работу примерно на неделю). Мейнфрейм обладает Сложностью 5 и стоит 200,000 $ плюс 1,000 $ за каждого пользователя. Он весит не менее 500 фунтов и занимает 6 кубических ярдов, не считая веса и размеров его терминалов и периферийных устройств.
Мегакомпьютеры: Такие системы обычно не доступны ранее TL9, хотя Мастер может ввести их в качестве сюрприза для игроков. Такие машины (их обычно называют "мегакомп") обладают Сложностью 7 и чаще всего применяются для управления уличным движением, канализацией, энергоснабжением и другими техническими функциями целого города! Они также выполняют всю канцелярскую работу для местных органов власти. Системы такого типа устанавливаются лишь в специально построенном для этой цели здании. Мегакомп питается от обычной сети, но наверняка будет иметь резервное питание из комплекса E-батарей (более 100 штук) и/или собственных генераторов на случай продолжительного отключения питания. Стоит такая система не менее 2,000,000 $, что делает ее недоступной для кого-либо кроме правительственных учреждений или больших корпораций (хотя владельцы иногда будут сдавать в аренду неиспользованное машинное время и дисковое пространство). Объем и вес мега-компьютера может быть самым разным, но самая простая модель весит как минимум одну тонну и занимает объем в 10 кубических ярдов.
Разумные компьютеры: Самое уникальное в мегакомпьютерах то, что потенциально они могут обладать самосознанием. Раз в год мастеру следует бросать 3d для каждой такой системы в кампании. Результат 6 или меньше означает ее "пробуждение". Недавно проснувшийся мегакомп может стать могучим союзником (или смертельно опасным врагом) для группы персонажей (см. "Компьютерные души", стр. 56 и "ИИ", стр. 83, для получения дополнительной информации). Когда компьютер становится разумным, его производительность немедленно возрастает до Сложности 8.

Использование компьютеров
При TL8 + все компьютеры могут иметь голосовой интерфейс; для большинства задач не требуется проверки на Программирование, а к умению Использование компьютера добавляется бонус +3.
Компьютер Сложности 2 может давать простейшие ответы; системы Сложности 4+ могут понимать идиомы и поддерживать нормальный разговор (в пределах своей области знаний, конечно). Программы распознавания и интерпретации речи дают возможность пользователю работать с компьютером и обеспечивают некоторую защиту (например, "не загружай эту таблицу и даже не признавай ее существование, пока не услышишь пароль 'Чабунагунга', произнесенный *моим* голосом"). Мастер обладает правом окончательного решения по поводу возможностей программы и действий компьютера, получившего определенное приказание. Простые системы могут быть опасны из-за буквального понимания ими речи.
Возможности компьютера зависят от его программного обеспечения. Не всякая программа может работать на любом компьютере. Программа Сложности 2 может работать на системе такой же Сложности или выше, но не может быть запущена на системе Сложности 1; но даже если это удастся, на скорость ее выполнения будет наложен существенный штраф (см. ниже "Программное обеспечение"). Максимальное количество программ, которое можно запустить одновременно, рассчитывается так: компьютер может выполнить две программы соответствующей ему Сложности или 10 программ более низкой; одну программу его Сложности и 5 программ более низкой. Возможности системы могут быть увеличены на 50 % (до трех программ собственной Сложности, 15 программ более низкой и т.д.) за 50%-ое увеличение ее цены.
Таким образом, компьютер Сложности 1 может выполнить две программы Сложности 1. Компьютер Сложности 2 может выполнить две программы Сложности 2, 10 программ Сложности 1, или одну - Сложности 2 и пять Сложности 1. Компьютер Сложности 6 может выполнить две программы Сложности 6, 10 программ Сложности 5, 100 программы Сложности 4 - и так до 100,000 программ Сложности 1, выполняемых одновременно! Так как большинство программ обладают Сложностью 4 или меньше, компьютеры Сложности 6 становятся очень мощными машинами.

Прозвища (Ники)
По очевидным причинам, большинство нетраннеров не желает использовать свои настоящие имена и анкетные данные в ходе работы. Вместо этого, большинство использует ник - псевдоним, который со временем становится их вторым именем (как в жизни, так и в сети).
Некоторые выбирают его без какого-либо обоснования, под влиянием момента. Другие мучаются над выбором целыми днями или даже неделями. Существует множество возможностей для выбора ника. Он может представлять собой как нормальное слово, так и остроумно (или не очень остроумно) измененное слово или каламбур.

Технологические: Это, наверное, самая популярная категория. Большинство нетраннеров - технофилы, и им нравится подчеркивать это своими никами. Например, Form Feed - "Подача страницы", Line Noise - "Помехи на линии", Deckmaster - "Мастер деки", Plug Head - "Штекер".
Философские: Некоторые из декеров - идеалисты, работающие из социальных, политических или религиозных убеждений. Например, Chicago 7 - "Чикагская семерка", The Libertarian - "Борец за свободу", Zen Master - "Мастер дзэн" и т. д.
Исторические: У многих нетраннеров есть любимый персонаж из истории или поп-культуры, которому они стремятся подражать. Тимоти Лири, Эбби Хоффман, Джон Леннон, Элвис, и т.д.
Литературные: Так же некоторые нетраннеры хотят походить на персонажей литературы, драматургии, кино и голографических фильмов: Эл Сид, Джордж Хэйдюк, Сирано, Генри Гондорфф, Том О' Бедлам, Добрая ведьма Гленда.
Образные: Множество ников попросту описывают образ, который нетраннер хочет создать: Network Ninja - "Сетевой ниндзя", Black Magic - "Черная магия" и т. д.

Аппаратура Tempest[1]
В конце 1980-ых была разработана аппаратура, способная получить данные, отображаемые на обычном терминале или мониторе, путем считывания его радиочастотного излучения. Она стала известна как аппаратура класса Темпест. Вскоре после ее изобретения любые правительственные системы, занятые обработкой секретных данных, обязаны были быть защищены от этого вида шпионажа - то есть их излучение должно было быть экранировано. Аппаратура класса Темпест дорого стоит - установка, которая позволяет персонажу считать данные с компьютерного дисплея на расстоянии в 100 ярдов стоит 500,000 $, весит 75 фунтов, занимает 1 куб. ярд и включает в себя монитор, антенну, и процессор.
Защита от такого нежелательного наблюдения увеличивает стоимость компьютера на 25 %, но в некоторых случаях она того стоит!

Следы
В обществе, где все больше возрастает значение компьютерной техники, все труднее становится сделать что-либо, не оставив за собой какой-либо электронный след. Некоторые нетраннеры специализируются в выслеживании людей по таким следам - можно сказать, что они ищейки эпохи высоких технологий.
Если нетраннер знает где смотреть - банковские данные, компьютеры правительства, и т.п. (и проникнет туда), он может перерыть системные базы данных в поисках ключа к местонахождению субъекта. Эта технология также известна как "сбор ссылок" на кого или "going GOTO" - выражение, пришедшее из языков программирования.
Мастер должен давать не текущий адрес и номер телефона субъекта (хотя благодаря критическому успеху при поиске в базе данных можно получить и такую информацию), а подсказки. Например - "Он купил авиабилет в Каир у турагента во Фресно".

Шифровка/Расшифровка
Важные данные, особенно редко используемые, часто хранятся в зашифрованном виде. Такая информация бессмысленна и бесполезна без соответствующей программы расшифровки.
Хорошая программа шифровки имеет Сложность 2 и стоит 1,000 $. На шифровку/расшифровку одного гигабайта данных в системе со Сложностью 2 нужен час (примените коэффициент 10 для более быстрых или медленных машин). Расшифровать данные обычно может только тот, кто знает ключ, который использовался для шифрования (подобно паролю). Если кто-то заполучил шифрованный файл, он может попытать счастья и подобрать ключ (особенно если он знает что-нибудь о придумавшем его человеке). Хакер должен бросить 3d и вычесть из результата 1, если он знает основную информацию (имя, адрес, имена родственников, и т.п.) человека, который зашифровал файл, и 2, если он хорошо его знает (на усмотрение Мастера). Если результат после вычитания становится равен 3, то хакер успешно подбирает ключ. Позволяются повторные попытки, но каждая следующая бросается (членами партии или теми, кого они наняли) с кумулятивным +1. Каждая попытка занимает 15 минут.
Программист, у которого есть доступ к мощному компьютеру (микрофрейму или более мощной системе), может написать программу для расшифровки информации. Это займет 1d дней, после чего нужно успешно выполнить проверку Программирования с -6.

Программное обеспечение
В игровых целях принято разделять два типа программ - аналитические и реального времени. К программам реального времени относятся, например, такие - Наведение на цель, Тяжелое вооружение, Пилотирование, Слежение за фондовой биржей и т. д., которые реагируют на происходящие события немедленно. Эти программы должны всегда работать без задержек - 5-секундная остановка при стрельбе из оружия в бою может закончиться плачевно. Аналитические программы включают в себя базы данных, Анализ внешней среды, Навигацию, и т.д. Их выполнение на системе такой же Сложности занимает около 10 минут.
Программа реального времени бесполезна на машине более низкой Сложности - она попросту не сможет работать достаточно быстро. Аналитическая программа может быть выполнена на машинах более низкой Сложности такого же TL, но каждая единица разности Сложностей в таком случае увеличивает время выполнения программы в 100 раз! Если у компьютера Сложность больше, это уменьшает время выполнения программы в 10 раз, но при этом она считается программой такой же сложности.
Пример: Составление курса программой Астронавигации Сложности 5 обычно занимает 10 минут. Оно заняло бы 1,000 минут на компьютере Сложности 4 и 10,000,000 минут на микрокомпе Сложности 2! Компьютер Сложности 6, выполняя ее как программу Сложности 6, проложил бы курс за одну минуту.

[1] TEMPEST - Transient ElectroMagnetic Pulse Surveillance Technology. Технология наблюдения за короткими электромагнитными импульсами. (Прим. перев.)

Хранение программ
При TL8 большая часть программного обеспечения хранится на дисках диаметром около трех дуймов, похожих на нынешние аудио компакт-диски (и использующие ту же систему поиска информации - в сущности, диск может иметь как звуковые дорожки, так и дорожки с данными). Каждый диск вмещает около 10 миллиардов байт (10 гигабайт, или гиг) данных. Чистый диск стоит 5 $ и десять дисков весят один фунт. Такие диски предназначены как для чтения, так и для записи данных, если они не "защищены от записи" - тогда их можно только читать. Софт также может быть "зашит" в микросхеме с пластиковым корпусом, которая подключается к стандартному разъему (слоту) кибердеки (см. стр. 75). Поскольку она размером с колоду карт, ее называют ПЗУ-картой (ПЗУ - это Постоянное Запоминающее Устройство, которое называется так потому, что с него можно лишь считывать, но нельзя записывать). ПЗУ-карта весит один фунт и подключается через компьютерный слот. У обычных компьютеров, в отличие от кибердек, всего один или два слота для ПЗУ-карт. Программа или база данных на ПЗУ-карте стоит на 50 % больше, чем такая же на диске, и изменение информации, хранящейся на карте, невозможно - но программы и базы данных с ПЗУ-карт выполняются вдвое быстрее, чем с диска. (Весь лед и другой защитный софт обычно хранятся на ПЗУ-картах) Подробнее о копировании ПЗУ см. "Защита от копирования", стр. 78, и "Запись ПЗУ", стр. 51.
По умолчанию количество слотов на всех обычных компьютерах (не кибердеках) равняется их Сложности. Эти слоты обычно используются для запуска льда (см. стр. 92). Увеличение стоимости компьютерной системы на 50 % удваивает их число, но дальнейшие увеличение их количества невозможно. Если у компьютера нет слотов, он способен выполнять любые программы кибердек с диска. Это удваивает время их выполнения, но на 25% уменьшает их цену (поскольку дешевле сделать диск, чем ПЗУ-карту).

Увеличение умений
Обычные программы дают персонажу бонус в +2 к соответствующему умению или поднимают его эффективный уровень до 12, смотря что выше. Этот результат может быть увеличен за деньги.
Удвойте стоимость программы за каждый дополнительный бонус +1 к ее умению или бонусу умения, который она дает. Например, программа Наведения на цель (Сложность 1, 5,000 $) с умением 12 могла бы получить умение 13 за 10,000 $, умение 14 за 20,000 $ или умение 15 за 40,000 $. См. "Чипы умений" на стр. 40.

Стандартные программы
Учет: Используется для проведения финансовых расчетов и прогнозов, и т. д. Сложность 2, 1,000 $.
Datalink (Программа обмена данными): Эта программа, которую также называют разумным терминалом, позволяет компьютеру связываться (через кабель или передающее устройство) с другим электронным устройством вроде портативного радара, сканера, и т.п. Соединившись через Datalink и посылая команды, компьютер может отображать данные с устройства и управлять им. Datalink также используется для общения с другими компьютерами через службы поиска информации. Сложность 1,400 $.
Ремонт электроники: Вместе со щупами из Комплекта инструментов для электроники (см. стр. 52) эта программа исследует любое электронное устройство с помощью встроенной технической базы данных. Сделайте бросок против умения программы, чтобы распознать поврежденный модуль; успех позволяет оператору понять, что и как нужно ремонтировать. Эта программа дает бонус в +2 к Электронике или Использованию электроники, или 12 в соответствующем умении, смотря что выше - но только для ремонта. Сложность 2,500 $. О технических базах данных см. стр. 67.
Проектирование: Это улучшенная инженерная программа CAD (автоматизированного проектирования). У каждой инженерной специальности есть собственная программа, которая дает премию +2 только к этому умению. Сложность 2, 5,000 $ плюс стоимость баз данных.
Экспертные системы: Это программы с экспертными знаниями в особых умениях, таких как Судостроение, Биохимия или Выживание в Арктике. Хотя им можно задавать вопросы из разряда "что - если", они вряд ли скажут что-то новое и, таким образом, не могут использоваться для оригинальных исследований или изобретений. Экспертные системы доступны для всех Профессиональных и Научных умений, а также для Выживания, Диагностирования и Анализа разведданных. Существуют также программы с черного рынка, распространенные в подполье, для умений вроде Компьютерного взлома.
Экспертные системы дают эффективное умение 12 для Ментальных/Средних умений, 11 для Ментальных/Сложных умений и 10 для Ментальных/Очень сложных. Они применяются вместо собственного умения персонажа, но время, потраченное на применение умения с помощью экспертной системы, удваивается. Экспертные системные программы имеют Сложность 3 и стоят 10,000 $ для средних, 20,000 $ для сложных, и 50,000 $ для очень сложных умений. Существуют экспертные системы и с более высокими уровнями умения; увеличение одного умения на единицу удваивает стоимость системы и увеличивает ее Сложность на 1. Утройте стоимость экспертной системы для любого нелегального умения.
Внутренняя безопасность: Эта программа контролирует и управляет внутренними системами безопасности здания или судна. Она или сама обладает умением 14, или добавляет +2 к умению оператора Использование электроники: Системы безопасности. Любой, кто пытается обмануть ее защитные датчики, должен выиграть Состязание умений: свое Использование электроники: Системы безопасности против умения программы. Сложность 3, 2,500 $.
Информационный демон: Эта программа постоянно просматривает каналы новостей в поисках сообщений и статей на заданную тему. Она может отложить их для просмотра позднее или немедленно предупредить пользователя о важном сообщении. Сложность 1,500 $.
Наведение на цель: При подключении к стационарной или смонтированной на шасси системе вооружений, эта программа дает стрелку +1 к умению Тяжелое оружие. Количество орудий в системе ограничено только возможностями программы; каждое требует отдельной копии программы в памяти (естественно, это могут быть копии оригинальной купленной программы). Компьютер должен иметь необходимые датчики и подключения (их стоимость обычно составляет 10 % стоимости оружия, или как минимум 500 $ за оружие). Сложность 1, 1,000 $.
Настольная издательская система: Используется для создания и обработки изображений и текстовых файлов, а также для проверки грамматики, правописания и стилистики. Сложность 2, 1,000 $.

Программы на заказ
При TL8+ систему можно запрограммировать на выполнение чего угодно. Конечно, качественное программирование стоит дорого при любом техническом уровне; мастеру следует позволить персонажам покупать программы на заказ, но они должны дорого стоить. Также не обойтись без серьезного тестирования, так как в такой программе при первом запуске наверняка найдется несколько забавных ошибок.
Если персонаж хочет написать собственную компьютерную программу, применяйте правила о Новых изобретениях (стр. B186), используя Программирование вместо инженерной специальности со штрафом умения, равным двойной Сложности программы, а не -15.

Базы данных
База данных - совокупность любой информации в электронном виде - от энциклопедии до личного списка адресов. При TL8+ у любой базы данных есть встроенные программы поиска и индексации. Для любой базы данных заданного размера справедливо утверждение, что чем более обширную тему она описывает, тем меньше в ней подробностей. Емкость базы данных измеряется в гигабайтах.
Один гигабайт информации может содержать что угодно из ниже перечисленного:
Общую информацию о приблизительно тысяче звездных систем; полные физические данные об одной такой системе; полную всемирную хронологию в общих чертах; ее же, но подробно, за период в 20 лет; годовые финансовые отчеты среднего бизнеса; полные досье на 100 человек с мельчайшими подробностями; большую книжную полка с любыми книгами; базу данных по переводу с какого-нибудь языка, со словарем, грамматическими правилами и подробными культурными ссылками.
Технические базы данных очень важны. Один гигабайт может содержать полное техническое руководство для космического шаттла или для десяти разных реактивных самолетов, или для 100 типов сложных транспортных средств, или для 1,000 простых (например, автомобилей), оружия или сложных электронных приборов, или для 10,000 технических схем разных устройств типа радио, магнитофона и т.п. (полные чертежи заняли бы в 100 раз больше места). Стоимость чипов с данными широко варьируется - коммерческие базы данных стоят тысячи, в то время как общедоступную информацию, такую как энциклопедия, можно купить за несколько сотен долларов. Секретная, специализированная информация, или жизненно важная либо очень ценная информация будет стоить гораздо дороже.

Чипы данных
База данных может быть сохранена на ПЗУ с помощью программатора ПЗУ (см. стр. 51). Это увеличивает стоимость базы данных на 25%, поскольку туда необходимо записать и софт для поиска данных. База данных на чипе (т.н. чип данных) работает в десять раз быстрее, чем если бы она находилась на диске.
Существует широкий ассортимент баз данных, доступных на чипах. Вот некоторые из наиболее интересных:
Коллекция вульгарных лимериков.
Британская энциклопедия.
Собрание сочинений Шекспира.
Полицейская картотека города на всех задержанных (доступна только офицерам правоохранительных органов).
Религиозные базы данных (Библия или Коран; *конкорданс Стронга*, и т.п.)
Трехгигабайтная база ***GURPS Basic Set*** четырнадцатой редакции.
Юридические книги.
"Анатомия" Грея (популярна у врачей).
Оксфордский словарь английского языка.
Чипами данных пользуются предприниматели, чтобы помочь своим клиентам. Общественные библиотеки, например, обычно держат свои каталоги на чипах, к которым можно подключаться, а в больших розничных складах часто есть стойки, у которых покупатель может найти нужную вещь, подключившись к чипу (обычно защищенному крепким кабелем).

Память большой емкости
В результате постоянного улучшения технологий, емкость памяти (жесткого или компакт-диска, и т.д.) увеличится настолько, что обычный пользователь никогда всю ее не заполнит. В игровых целях считайте, что стоимость компьютерной системы включает в себя объем памяти, достаточный для одновременного выполнения максимально разрешенного Сложностью системы количества программ (см. ниже).
Однако системы, на которых выполняются программы по обработке действительно огромных массивов данных, потребуют дополнительной памяти. Если система должна поддерживать базы данных более чем (Сложность x 100) Гб., ей потребуется дополнительная память большой емкости. При TL8, один терабайт (один триллион байтов, или 1,000 Гб.) защищенной памяти стоит 10,000 $, весит 500 фунтов и занимает приблизительно 1 куб. ярд.

Цифровая сеть с комплексными услугами (ISDN[2])
Поскольку сеть становится все более сложной, скоро исчезнут линии, предназначенные исключительно для телефонной связи или только для передачи данных. Вместо этого в сети будут существовать широкополосные сигналы, способные передавать одновременно аудио- и видеосигнал (двух - или трехмерный) в реальном времени. Если сеть кампании достаточно современна, по ней можно будет передавать нейроимпульсы, управляющие вкусом, обонянием, осязанием, и т.п.
Информация об источнике и адресате также может быть легко закодирована в передаче ISDN сети. С одной стороны это позволит получателю выбирать, от кого он разрешает входящие передачи (особенно, если это счет, связанный со сделкой), а с другой - позволит торговцам отслеживать, кто именно прибегал к их услугам и выставлять соответствующие счета. Это приведет к массовой реорганизации компьютерных и сетевых услуг.

[2] ISDN - Integrated Services Digital Network

Некоторые услуги, перечисленные здесь, уже доступны в 1995 (плата за просмотр фильмов и спортивных состязаний, интерактивные телевидение и видеофоны), в то время как другие технологически возможны, но пока не распространены (музыка, издательство, игры).

Кино: Вместо того чтобы платить за посещение кинотеатра, киноманы смогут посмотреть прокатные фильмы дома. Цена будет начисляться за каждый просмотр - если фильмы не защищены от копирования, дистрибьюторы, вероятно, назначат цену из расчета возврата своих вложений уже за время первых же просмотров.

Интерактивное телевидение: Эта услуга частично доступна уже в 1990-ых. Зрители способны влиять на решения, сделанные персонажами их любимого ТВ или Три-ТВ шоу путем голосования в опросах создателей шоу. Сетевые покупки станут более распространены, поскольку покупатели смогут, листая гипертекстовые меню и каталоги, посмотреть на одежду или вещь и изменить ее цвет или стиль. С применением голографии можно будет даже "примерить" одежду по сети - ее трехмерное изображение будет проецироваться прямо на тело.

Издательство: Так как цены на лазерные принтеры постоянно снижаются, скоро они станут стандартным периферийным устройством. Издательский рынок будет быстро расти, поскольку прежние тиражи в 100,000 экземпляров станут ненужными. Вместо этого читатель загрузит текст в лазерный принтер, распечатает его и склеит готовую книгу (клей также недорог). Если цены на цветную полиграфию продолжат снижаться, читатель сможет даже скопировать обложку и внутреннее оформление книги!

Игры: Уже существующие интерактивные сетевые игры, доступные через коммерческие компьютерные сети в 1990-ых, характеризуются ограниченными графическими возможностями (т.н. псевдографика) и низкой сложностью. С появлением широкополосной интерактивной связи игровое моделирование может достичь новых высот. Представьте себе фентэзийную ролевую игру, участники которой, находясь в разных уголках страны, видят перед собой экран, где местность и остальные персонажи транслируются в реальном времени (или передаются непосредственно в мозг, если доступна технология нейро-интерфейсов!). См. "Игры-грезы" на полях.

Связь: Звоня друг другу, люди будут видеть своего собеседника на видео- или голографическом дисплее. Естественно, можно будет отключать такую возможность, если вы, скажем, находитесь в душе!

Кроме того, будет намного проще пригласить к обсуждению двух, трех или большее число людей - при этом каждый будет занимать свое "окно" на экране.

Музыка: С появлением больших и дешевых устройств хранения музыки при скорости передачи данных 5 Мб/сек. средний компакт-диск можно будет загрузить за 90 секунд. Здесь все во многом аналогично кино- и издательским услугам.

Так же будут возможны интерактивные джем-сейшены, когда музыканты, находящиеся далеко друг от друга, будут встречаться для совместной игры. Подключив MIDI (цифровой интерфейс музыкальных инструментов), артисту даже не обязательно быть на том континенте, где находятся его инструменты!

Игры - грезы

Эти интерактивные имитации, также известные как "иллюзии", обладают одновременно размахом и бюджетом кино-бестселлера, а также дают возможность непосредственно действовать, словно в аркадной игре, в виртуальной реальности, воздействующей на все органы чувств. Для них нужен нейро-интерфейс, поэтому они могут быть недоступны в некоторых кампаниях. Пользователь просто подключает разъем, запускает имитацию и становится героем истории.

Самые популярные виды игр-грез - приключенческие истории, готические романы и порнография. В таких играх софт моделирует личности каждого персонажа, кроме героя, а отлично проработанная графика делает изображение и эффекты захватывающими и всеобъемлющими. Все сосредоточено на герое, и сюжет, стремительно развиваясь от сцены к сцене, поддерживает на высоком уровне увлеченность пользователя и адреналин в его крови.

Сюжет игры может включать в себя от десятков до сотен эпизодов общей продолжительностью 30 - 60 минут. У самых сложных игр-грез может быть несколько дополнительных и альтернативных сюжетных линий, что дает пользователю ощущение участия в принятии решений. У программы есть небольшие уловки и подсказки, позволяющие наставить на путь истинный: в нескольких ключевых местах есть "тупиковые ветки", которые говорят о том, что герой принял неправильное решение и предоставляют ему правдоподобную возможность вернуться к правильному сюжету. Другие разработаны как "история с минимальными возможностями", с единственной сюжетной линией длительностью от полутора до шести часов. В них сюжет имеет четкую кульминацию и развязку, хотя у некоторых есть множество продолжений.

Связанные с ними "имитации-грезы", в которых применяется та же самая технология, разработаны, чтобы сосредоточиться на отдельном типе деятельности и обучить пользователя определенному умению. Хотя они и остаются очень интересными и увлекательными, они не так запутаны, как игры-грезы. Поскольку их сюжеты проще, элементы имитации можно бесконечно комбинировать, замкнув грезу и продолжая ее нужное время. Для примера можно привести популярные "Интерактивный семинар по менеджменту" и "Шоссе 666" (симулятор вождения автомобиля). Имитации вроде "Симпозиума по геологии", являются сугубо образовательными, но даже учебный процесс может быть приятным; "Фараон" - имитация управления ресурсами, созданная, чтобы показать игроку всю сложность управления большим государством, дарует игрокам чувство власти от отправки огромных армий и управления судьбами тысяч людей!

Игры-грезы могут вызвать привыкание; чтобы избежать его, пользователь должен делать бросок на Волю за каждый полный час имитации, с -1 за каждый час без перерыва (в данный конкретный день). Игры довольно дороги и привыкание к ним будет стоить -15 очков. Имитации-грезы безопаснее, даже наиболее увлекательные из них требуют броска на Волю каждые два часа, а многие другие и того реже. У персонажа также может существовать Заблуждение насчет реальности грез и иллюзорности действительности; если это лишь сомнения, то это Заблуждение на -10 очков, а если персонаж уже не верит в действительность окружающего мира, считая его сном, это будет серьезным Заблуждением на -15 очков.

Другим повальным увлечением будет интерактивная порнография. Эта услуга позволит пользователю выбирать из широкой палитры сексуальных фантазий все, что может быть сымитировано электроникой - максимально безопасный

секс. Если компьютер, предлагающий эту услугу, будет обладать достаточной мощностью, то она будет обладать интерактивностью вместо заранее запрограммированного сценария. Персонаж с недостатком Развратность получает штраф в -4 на броски Воли с целью избежать привыкания.

Развитие Сети
К концу 1980-ых уже существовала развитая всемирная компьютерная сеть. Американские сети пакетной коммутации типа GTE Telenet обеспечивали доступ к тысячам компьютеров во всем мире, типа Dacom-Net в Южной Корее, Venus-P и DDX-P в Японии, Datapac в Канаде, Isranet в Израиле и многих других (см. поля, стр. 70-71). Любой пользователь с правильной NUI (сетевой пользовательской идентификацией), мог подключиться к этим сетям.
Существует также множество различных компьютерных сетевых и информационных служб в пределах Соединенных Штатов - от бесплатных общедоступных сетей типа USENET и платных, таких как CompuServe и MCI Mail, до любительских BBS-сетей (BBS - электронная доска объявлений) типа FIDOnet и WWIVnet Вейна Белла. Эти сети позволяют системным операторам (сисопам) и пользователям совместно пользоваться информацией и посылать почту пользователям BBS в разные системы другого города, штата, страны или мира.

Типы узлов
Есть три различных типа узлов в компьютерной сети: публичные, обычные и защищенные.
Публичный узел позволяет любому, кто этого хочет, подключится к нему, обычно через гостевой аккаунт, который не требует пароля. Они включают в себя общедоступные почтовые системы, открытые базы данных и многоканальные чаты.
Обычные узлы составляют основную часть сети. Это частные системы (деловые, правительственные или учебные) со стандартной защитой. Чтобы подключится, каждому пользователю нужен пароль, и каждый день или неделю ведется учет, призванный определить пользователей системы.
Защищенные узлы принадлежат людям, которые, чтобы предотвратить несанкционированный доступ, принимают активные меры вроде подключения модемов обратного вызова, идентификации линии абонента и скрытых файлов паролей. Эти узлы обычно содержат правительственные или корпоративные системы высокого уровня, или информацию, которой легко злоупотребить (компьютеры АТС, списки счетов крупных компаний, системы министерства обороны, и т.д.).
Дополнительную информацию о проектировании сети см. в разделе "Отображение Сети", стр. 82.

Уровни доступа
В этих правилах для простоты используются только два уровня доступа - обычный и привилегированный. Мастер, желающий большего реализма, может добавить любое количество уровней доступа к компьютеру - нетраннер никогда не знает, чью учетную запись (аккаунт) он взломал! Некоторые из наиболее распространенных аккаунтов:
Гостевой или демонстрационный - разрешает войти кому угодно без ввода пароля, но позволяет выполнять лишь очень ограниченный набор команд. Стандартными командами могут быть: связь с системным оператором, отправка электронной почты, чат с другими пользователями, просьба о нормальном аккаунте и запуск рекламного ролика о работе компании. Promote получает -4 при запуске с такого аккаунта, поскольку они обычно защищены от действий такого рода.
Руководитель проекта - может принадлежать начальнику инженерной группы или преподавателю колледжа. Это дает пользователю полный контроль над аккаунтами своих подчиненных, но никакой власти над посторонними. Как правило, однако, он имеет право создавать обычные учетные записи. Promote получает +1 при запуске с такого аккаунта.
Ассистент оператора - этому аккаунту один шаг до привилегированного. Он позволяет быть всюду и просматривать что угодно, но не разрешает изменять или удалять не принадлежащие ему файлы. Создавать и удалять учетные записи обычно можно. Promote получает +3 при запуске с такого аккаунта.
Специальные учетные записи - многие учетные записи создаются для выполнения единственной функции. Если брать пример из наших дней, то аккаунт "uucp" в системе Unix существует только для того, чтобы копировать файлы с машины на машину. Их слишком трудно использовать в посторонних целях, поэтому Promote получает -4 при запуске с таких аккаунтов.

Компьютерная безопасность
Приключенцы могут пожелать проникнуть в компьютерную систему - обычно для того, чтобы украсть, изменить или уничтожить информацию, хотя иногда - просто осмотреться (или доказать, что они на это способны). Для этого они должны иметь доступ к системе - или через специализированный терминал или через использование Datalink (стр. 65). В полностью изолированную систему нельзя проникнуть снаружи, но таких систем немного (см. "Развитие Сети" выше).

Обычные и привилегированные пользователи
В игровых целях используются два типа учетных записей, установленных в системе - аккаунты обычных пользователей и аккаунты с большими правами т.н. привилегированных пользователей (если мастеру нужно больше уровней доступа, см. поля на стр. 68). Естественно, каждый хакер хочет заполучить такой аккаунт, поскольку привилегированные пользователи имеют доступ ко всей системной информации.
На практике получить доступ к такой учетной записи гораздо сложнее, чем к обычной. Системные администраторы (сисадмины) осторожнее подбирают им пароли и внимательно следят за использованием таких аккаунтов.
Когда нетраннер успешно проникает в систему, мастер должен скрытно бросить 3d. Результат 7 или меньше означает, что ему достался привилегированный аккаунт. Конечно, если персонаж пытается взломать известную ему учетную запись, которая имеет такие привилегии (принадлежащая системному оператору, например), бросок не нужен - но попытки взлома известного привилегированного аккаунта совершаются с -2, поскольку эти аккаунты обычно лучше защищены. Все попытки получить или изменить информацию, сделанные через такую учетную запись, получают +2.

Если персонаж проник в систему под обычным аккаунтом, он может попробовать написать программу, которая поднимет его статус до привилегированного. Для этого нужно 5d минут и успешная проверка Программирования или Компьютерного взлома -3. Данная проверка получает -2, если это публичная система, -4 если обычная и -8 если защищенная. Если проверка провалена, пользователь может попытаться снова; каждая попытка делается с кумулятивным штрафом в -1. Если персонаж терпит неудачу пять или больше раз, будет сделана некая отметка или поднята тревога - кто-то узнает, что он был там! Мастеру следует делать эти проверки в тайне.

Попадание внутрь системы

В сетях защита почти полностью основана на паролях и идентификационных номерах. Их можно получить разными методами. Самый простой путь - попытка "грубого взлома". Исследования показали, что набору из 100 распространенных паролей соответствует почти 20% учетных записей пользователей. Такие слова как "тайна", "пароль", "Эйнштейн" и т.п. используются снова и снова, как, впрочем, и номер карточки социального обеспечения, имена жен или мужей и другая легко доступная информация. При первом входе в "обычную" систему (см. "Типы узлов" на стр. 68), мастер должен позволить игроку сделать бросок против умения Компьютерный взлом -5. Удача говорит о том, что персонаж нашел один из таких "простых" паролей. Этот бросок предполагает, что он знаком с типом компьютера, в который пытается проникнуть, но ничего не знает о его пользователях. Если нетраннер сталкивается с неизвестным ему компьютером (мастеру следует составить список известных производителей в кампании), то все попытки взлома совершаются с -2, пока он не проникнет в такую же систему. Если персонаж знает основную информацию об одном или более пользователях системы (имена, адреса, имена родственников, увлечения, и т.д.), попытка взлома совершается с +2.

Такая попытка взлома займет 2d минуты; их может быть несколько (по мере того как взломщик придумывает новые, более подходящие пароли), но каждая последующая делается с дополнительным пенальти -3.

Для взлома "защищенных" систем нужно быть гораздо хитрее. Их пароли обычно генерируются компьютером и представляют собой случайную комбинацию символов и чисел, например, "ATX10Y9". Их невозможно отгадать. Кроме того, иногда эти системы настраиваются таким образом, что разрешают вход только с отдельных узлов и только в определенное время.

Персонаж, пытающийся взломать защищенную систему, должен сделать проверку на Компьютерный взлом -10, чтобы определить, стал ли кто-то жертвой своей небрежности (или удачи хакера). Успех показывает, что он вошел; 3 или 4 - что он вошел как привилегированный пользователь. Возможны множественные попытки взлома, как и для обычных систем.

Конечно, кроме взлома "в лоб" есть и другие способы войти в защищенную компьютерную систему. Один из них заключается в перехвате потока данных легального пользователя; обычно это достигается подключением в качестве привилегированного пользователя к незащищенному узлу между легальным пользователем и его адресатом и успешным броском на Компьютерный взлом.

Пример: Джон Смит - легальный пользователь защищенного узла Гамма, принадлежащего ФБР. Он работает на компьютере в своем офисе (узел Альфа). Во время подключения к Гамме поток его данных проходит через обычный узел Бета. В это же время Дэк Визард (персонаж-хакер) получил доступ к Бете в качестве привилегированного пользователя. Он делает проверку на Компьютерный взлом, который у него равен 15, и выбрасывает 9; нет проблем. Теперь он может контролировать любую информацию, проходящую через Бету - включая все, что вводит Джон Смит (например, номер его учетной записи и пароль)! Другой метод добычи информации хакеры называют "социальной инженерией" - что также известно под названием обман. Хакер звонит или посещает компанию, контролирующую нужный узел и выдает себя за того, кто обладает легальным доступом к компьютеру, например, за сетевого инженера или служащего, находящегося в командировке. Это трактуется как состязание умений: Заговаривание зубов персонажа против IQ NPC. Мастер должен применять модификаторы, зависящие от уровня знаний персонажа о компьютере и компании, к которым он применяет этот метод. У бывшего работника телефонной компании будет существенное преимущество при попытке обмана такой же компании перед кем-то, кто никогда не видел телефонной аппаратуры сложнее телефона-автомата! В общем случае любой, кто пытается применить социальную инженерию, должен обладать навыками Программирования 10+, электронной или компьютерной инженерной специальностью 10+ или Компьютерным взломом 10+, чтобы успешно выдать себя за специалиста по компьютерам. Без этих предпосылок Заговаривание зубов получает штраф -4. Мастер может заменить эти предварительные условия другими умениями.

Наконец, есть программы, которые помогают получить несанкционированный доступ к системе (см. "Программное обеспечение кибердек" на стр. 88). Они используются для проникновения через системную защиту и описываются ниже, в разделе "Киберпространство". Если мастер против существования множества доступных программ такого рода, для обычного проникновения в систему достаточно навыка Компьютерного взлома. См. поля на стр. 78 для получения дополнительной информации о быстрой обработке взлома.

Что дальше?

Как только взломщик проник в систему в качестве легального пользователя, он может попробовать добиться доступа к ее программам или базам данных. Некоторые базы данных доступны для любого пользователя, в то время как другие защищены специализированными программами типа Datalock (см. стр. 93) и требуют паролей. Например, в компьютерной системе военной базы у пользователя будет доступ к множеству баз данных. К некоторым из них, вроде биографий старших офицеров из отдела связей с общественностью, доступ будет свободным. К другим, таким которые, например, касаются советников по строительству секретных объектов, доступ будет ограничен и вызовет тревогу при обнаружении попытки несанкционированного доступа.

Каждая попытка занимает пять минут. Успех означает взлом защиты и удачное проникновение. Если это была попытка взлома базы данных, теперь у взломщика есть к ней доступ - т.е. возможность изменения, удаления или поиска нужной информации. Если это была программа, он может попытаться перепрограммировать ее.

Провал на 1 или 2 означает, что попытка потерпела неудачу, но можно попробовать еще раз, потратив еще пять минут; провал на 3 и более означает, что защита компьютера, если она есть, подняла тревогу - см. "Программное обеспечение кибердек".

Мощный компьютер может хранить тысячи гигабайт информации в базах данных, и найти нужный объект в таком случае будет сложно. Например, поиск в досье 5,000 служащих компании человека, который когда-то служил в 4905-ом минометном взводе морской пехоты, может занять много времени, а чем больше его потрачено на нелегальный поиск, тем больше вероятность активизации тревоги. Чтобы осуществить поиск, определите размер исследуемой базы данных перед проверкой на Использование компьютера.
Штраф -1 для баз данных размером до 10 Гб., -2 - от 11 до 100 Гб., -3 - от 101 до 1,000 Гб., и т. д. Например, если полные досье на 100 человек занимают 1 Гб., то для 5,000 человек понадобится 50 Гб., и поиск получает штраф -2.
Каждая попытка поиска требует 10 минут на 1 гигабайт. Если она осуществляется нелегально, критический провал приводит к активации защитных программ системы (если они есть). При легальном поиске каждая попытка все равно занимает 10 минут на 1 гигабайт и получает такие же штрафы за размер базы данных. Неудача просто означает, что поиск не дал результата - без ограничений по времени можно найти что угодно! Конечно, такой информации может там и не быть - это решает мастер. Персонажи могут понять, а могут и не догадаться, что их поиск бесполезен. Представим, например, что в описанной выше ситуации не существует служащего, который раньше служил в этом взводе морской пехоты. После первой попытки поиска, успешной или нет, мастеру просто следует объявить, что такой служащий не найден. После нескольких попыток (или одной, которая была бы успешной, если бы такой работник был), мастер может сказать, что все данные были просмотрены, и такого человека не существует.
Большее количество доступных действий после проникновения в систему описано на стр. 79.

Взлом и защита при отсутствии киберпространства
Мастер должен просмотреть список программ для кибердек (стр. 88) и определить, какие из них будут работать в его сети. Вместо использования Командных этапов применяйте ходы, в зависимости от времени выполнения (например, программа со временем выполнения 2 требует 2 хода для активизации). Программы будут представлять информацию в виде текста или пиктограмм (иконок), и некоторых видов льда (вроде Flatline) не будет.

Изменение программы и "черный ход"
Пользователь, полностью контролирующий систему, может изменить любой ее софт. Когда программу безопасности изменяют с целью облегчить хакеру взлом системы, это называется "оставить черный ход". Постоянный кошмар штатных сотрудников безопасности - опасение, что разработчик их защитных программ оставил для себя пару таких ходов про запас. Такое бывало.
Чаще всего черный ход представлен в виде небольшого дополнения к программе аутентификации. Любого, кто знает пароль к нему, измененная программа будет игнорировать или считать легальным привилегированным пользователем. Само существование черного хода делает программу более уязвимой и предоставляет хакеру дополнительный вход. Программа с большим количеством таких ходов быстро обесценивается.
Персонаж может создать черный ход. Трудность этой задачи обратно пропорциональна тому, насколько просто сисадмину определить ее местоположение. Простейший случай требует броска на Программирование или Компьютерный взлом -2. Один раз в неделю мастер должен бросать 3d. При 10 или меньше ход был обнаружен. За каждые -2 к броску умения при его создании от броска на его обнаружение вычитается 1.
Пример: хакер заявляет, что он попытается создать черный ход, который будет заметен при 6 или меньше. Поскольку это на 4 меньше чем обычно, потребуется успешная проверка против Программирования -8 или Компьютерного взлома -10.

Чаты
Одной из самых популярных систем в сети будут конференции в реальном времени - т.н. чаты. Это узлы с большим количеством входных линий, которые позволяют пользователям связываться (открыто или конфиденциально) друг с другом.
Хакеры обычно используют чаты для обсуждения будущих целей или торговли информацией. Опасность состоит в том, что никто не может быть точно уверен, с кем разговаривает.
В хакерских чатах нашего времени (например, Altgers в Западной Германии и QSD во Франции) используются сложные протоколы для общения друг с другом. Туда входят кодовые фразы для начала беседы, отказ от "настоящих" имен, и много других методов обеспечения секретности.
Вторая опасность чатов состоит в том, что пользователи должны доверять его администрации. Если нетраннер пользуется незнакомым чатом, Мастер должен бросить 3d. При 7 или меньше разговор отслеживается и возможно, записывается. Что происходит потом - забота мастера.

Названия сетей
Во многих кампаниях по киберпанку мастеру достаточно описать просто "Сеть" - глобальную, всеобъемлющую, покрывающую земной шар целиком. Однако если мастер хочет большей детализации, ниже приведен перечень сетей 1990-ых. И хотя некоторые из них исчезнут и появятся новые, этого должно быть достаточно, чтобы внести "разнообразие" реальности в кампанию.

Название страны	***Сеть***
Аргентина	Entel
Австралия	AustPac, Midas
Австрия	RadAus
Багамы	BaTelco
Бахрейн	BahNet
Барбадос	IDAS
Бельгия	DCS, EuroNet
Бермуды	C&W
Бразилия	InterData

Канада	Datapac, GlobDat, Infoswitch
Каймановы острова	C&W Cayman
Китай	PKTelcom
Колумбия	Dapaq
Коста-Рика	RacsaPac
Дания	Datex, DataPak
Доминиканская республика	UDTS
Египет	Arento
Финляндия	Datex, Datapak, Digipak
Франция	TransPac,TI, EuroNet
Французские Антильские острова	TransPac
Французский остров Гваделупа	DomPac
Французская Мартиника	DomPac
Французский остров Реюньон	DomPac
Габон	GabonPac
Германия	EuroNet, Datex-P
Греция	HelPak
Гондурас	HonduTel
Гонконг	IDAS/ITS, IntelPak, DAS, DataPak
Венгрия	CTO
Исландия	ICEP
Индонезия	SKDP
Ирак	IDAS
Ирландия	IPSS, EuroNet, EirPac
Израиль	IsraNet
Италия	Dardo, EuroNet
Кот-д'Ивуар	SystranPak
Ямайка	JamanTel
Япония	DDX-P, NIS/Tymnet, Venus-P
Южная Корея	DacomNet, Dacom
Люксембург	EuroNet, LuxPac
Мексика	TelcPac
Нидерланды	DataNet, EuroNet, Dabas
Новая Зеландия	IPSS
Норвегия	Datex, DataPak
Панама	Intel
Перу	Etel
Филиппины	ETPI, UDTS, PGC
Португалия	SABD
Катар	IDAS
Саудовская Аравия	IDAS
Сингапур	TelePac
Южная Африка	SAPONet
Испания	IberPac
Швеция	TelePac, DataPak
Швейцария	TelePac, DataLink
Тайвань	PacNet, UDAS
Таиланд	IDAR, CAT
Тринидад и Тобаго	TexTel
Объединенные Арабские Эмираты	Tedas
Великобритания	IPSS, PSS, EuroNet, Mercury
США	WUT, UDTS2, Datel I и II, Telenet, Tymnet, ARPAnet, Infomaster, GraphNet, TRT, FTCC, UniNet, Autonet, CompuServe, GENIE, AlaskaNet, JANET, Internet
Гуам	RCA
Пуэрто-Рико	UDTS, RCA/PR, PRTCC
Виргинские острова	UDTS

КИБЕРПРОСТРАНСТВО

Представьте себе черную пустоту, заполненную мерцающими светящимися точками, каждая из которых представляет собой самородок данных, более ценных, чем золото. Неоновые линии сети сходятся в узлах связи, а светящиеся ленты данных летят ввысь, чтобы подключиться к хромированным спутникам.
Это - киберпространство, мир опытных нетраннеров - воров данных, которые входят в сеть, рискуя, что их мозги окажутся изжарены как яичница, чтобы сорвать полумифический "большой куш" и увековечить себя. Конечно, некоторые не гоняются за деньгами - они чувствуют буквально наркотическую зависимость от острых ощущений и адреналина, затопляющего нервную систему. Говоря проще, они подсели...

Нейро-интерфейсы
Изобретение нейро-интерфейса (см. ниже) возвестило о наступлении новой эпохи. Вместо ограничений, присущих медленной клавиатуре, неудобной мыши или неточной системе распознавания речи, опытный пользователь теперь мог мысленно управлять компьютером.
Самые первые нейро-интерфейсы были соединены с оптическим нервом и мускулами вокруг него. Интерфейс проецировал данные непосредственно в оптический нерв; пользователь "видел" бегущую строку текста, как в кино или на торгах. Все команды отдавались голосом.
Во втором поколении использовался графический, или *иконный*, интерфейс. Вместо отданного голосом приказа показать файл, например, пользователь видел изображение файла, который можно было открыть или закрыть мысленной командой. Это существенно увеличило скорость доступа к данным.
Вершиной развития интерфейсов стал *пространственный* интерфейс - полностью трехмерный "мир", в котором все системы и данные были представлены объектами, с которыми можно взаимодействовать в реальном времени. Теперь вместо того, чтобы мысленно скомандовать "открыть", смотря на файл, пользователь мог просто взять этот файл своими воображаемыми "руками" и пролистать его.
Мастер в киберпанке может выбрать любую степень технического развития своей кампании. Больше всего это повлияет на стоимость интерфейса и скорость выполнения им команд или программ. Все цены, приведенные ниже, даны на момент появления соответствующего оборудования. Цена "старых технологий" на 50% меньше за каждую новую их степень, появившуюся в игре. Таким образом, Текстовый интерфейс стоит 50,000 $ на момент начала его производства, но только 25,000 $, если уже доступен Графический и 12,500 $, если уже существует Пространственный интерфейс.
Такая же прогрессия применяется к очкам персонажа, если мастер требует заплатить ими за эти технологии.
Всем нейро-интерфейсам для подключения к сети нужна кибердека (см. ниже).

Текстовый интерфейс 50,000 $ (20 очков)
Это самый примитивный нейро-интерфейс. Вся информация представляется в текстовом виде, и все команды подаются голосом. Для его установки требуется как минимум двухнедельное пребывание в крупном хирургическом учреждении. Программа Datalink (см. стр. 65) может быть встроена в него (как и в любой интерфейс следующего поколения) за дополнительные 1,000 $ (умение программы может быть улучшено до нормального). Командный этап занимает в 4 раза больше времени при использовании Текстового интерфейса (см. "Командные этапы" ниже).

Графический интерфейс 80,000 $ (25 очков)
Этот интерфейс очень похож на операционные системы на основе пиктограмм (иконок), используемые на персональных компьютерах в 1980-ых и начале 1990-ых. Двумерный "экран" проецируется непосредственно в оптический нерв персонажа. Когда он хочет выполнить программу или исследовать базу данных, он мысленно "выбирает" соответствующую иконку. Например, чтобы соединиться с другим компьютером, он выбирает изображение телефона; чтобы отключиться от системы - значок двери. Иконки могут быть индивидуальны - например, хакер может использовать изображение индюшки для обозначения плохо защищенного компьютера.
Его установка требует как минимум десять дней пребывания в крупном хирургическом учреждении. При использовании такого интерфейса командный этап занимает вдвое больше времени.

Пространственный интерфейс 100,000 $ (30 очков)
Это последнее достижение в области нейро-интерфейсов. Когда персонаж подключается к сети, он видит завершенный и детальный мир вокруг себя. В некоторых кампаниях будет существовать только один вариант визуального отображения сети; в других персонажи смогут подключить к своей кибердеке разные Пространственные модули, и, наконец, некоторые версии киберпространства позволят нетраннеру интерактивно создавать свое Пространство, изменяя его при необходимости (см. стр. 88).
Его установка требует двух недель пребывания в крупном хирургическом учреждении, плюс еще две недели "пространственной ориентации" (обучение использованию нейро-интерфейса и кибердеки) и неделю на каждый вид Пространства, с которым персонаж хочет ознакомиться. При использовании этого интерфейса Командный этап имеет стандартную продолжительность.

Защита информации
Итак, если компьютерные системы настолько просто взломать, как персонажи смогут скрыть свою информацию от любопытных глаз? Ответ, естественно - никак. Методы, которые они используют для взлома чужих систем, могут применить и к ним. Можно уменьшить вероятность кражи данных, храня их на съемных носителях (вроде дискет), но это не всегда приемлемо или возможно. Зачастую персонажам будет нужно (или захочется) хранить секретные данные в Сети. В таких случаях игрок должен описать действия персонажа по защите данных. Например, можно сказать мастеру пароль, который персонаж использует для доступа к своим данным. Тогда мастеру следует назначить модификатор на любую попытку взлома учетной записи персонажа, основанную на сложности пароля. Пароль типа Z4Z!230N5 будет намного тяжелее угадать, чем, например, GURPS:GAMER. Но после этого каждый раз, когда персонаж захочет получить доступ к своему аккаунту, мастер должен заставлять игрока вспоминать пароль! Если он ошибется хотя бы в одном символе, то не сможет войти, а если он где-нибудь запишет пароль, мастер может решить,

что кто-то его украл и получил доступ к аккаунту! Извлечение данных, закрытых забытым паролем и защитными программами, которые без него не пустят внутрь даже установившего их человека, может развлечь вас на весь вечер. Другие меры, которые можно предпринять, включают в себя обработку в бумагорезательной машинке всех выбрасываемых документов, имеющих отношение к системе, а также физическую защиту (установку замков и сигнализации) компьютера и линий связи, к которым он подключен.

Физическое повреждение систем

Большинство хакерских программ создаются для работы с софтом. Они крадут или изменяют данные, блокируют программы защиты и т.д. Они не работают с "железом".

Большинство документации XX столетия утверждает, что программы или команды с клавиатуры не могут разрушить аппаратную часть компьютера, что очень успокаивает неопытных пользователей. Но это не совсем так.

Любая команда, которая зацикливает движения какой-либо части аппаратуры, может повредить ее. Относительно безопасный пример (это распространенная в колледже шутка) - программа, которая посылает на принтер ряд команд перехода на новую строку... после чего на полу образовываются горы бумаги. Более разрушительной, например, будет программа, заставляющая циклически двигаться жесткий диск, пока он не сотрется в пыль или не загорится.

Но хакер не сможет написать такую программу, не зная точно, какое "железо" он атакует. Даже зная все, что нужно, из-за встроенной защиты эта задача потребует не менее недели и проверки на Программирование с -4 или хуже. И протестировать такие программы до их непосредственного применения тяжело! Но они могут вызвать большую шумиху, и если программист выполнит проверку на 3 или лучше, повреждения вначале будут выглядеть простой аппаратной неисправностью.

Конечно, это потребует изрядной ловкости со стороны атакующего. Есть и другие способы сделать то же... например, заставить систему безопасности дать охране команду стрелять во всех находящихся в машинном зале!

Командные этапы

Когда пользователь подключен с помощью интерфейса к кибердеке, каждое его действие занимает несколько Командных этапов (или просто этапов). Время выполнения Командного этапа зависит от типа нейро-интерфейса, Сложности и качества кибердеки, а также от умения нетраннера. В то время как 100 миллисекунд - одна десятая секунды - это не слишком долго для большинства людей, для нетраннера они могут стать вопросом жизни и смерти!

При средней продолжительности этапа в 1,000 - 2,000 миллисекунд для быстрейших операторов человечества на лучших кибердеках он длится 100 миллисекунд, а ИИ может достичь скорости в 10 миллисекунд...

Среднее быстродействие компьютеров

Продолжительность Командного этапа зависит от Сложности компьютерной системы или кибердеки. В некоторых системах ради большего быстродействия увеличивают мощность процессора - удвоение обычной цены компьютерной системы уменьшает продолжительность этапа на 25 %.

Сложность системы	Продолжительность этапа (в миллисекундах)
1	16,000
2	8,000
3	4,000
4	2,000
5	1,000
6	500
7	200
8 (только для ИИ)	100*

*У неигрового персонажа-ИИ этап может длиться и 10 миллисекунд - мастер задает его по своему желанию!

Социальная значимость нейро-интерфейсов

Даже если нейро-интерфейсы станут широко доступны, не каждый захочет установить себе их. Причина более чем серьезна - немногим нравится мысль о ком-то, копошащимся в их мозгу, вне зависимости от профессионализма доктора или техника и заманчивости результата. Другие будут думать, что это вполне естественно, и к началу эры киберпанка "компьютерные мозги" будут почти в каждой профессии:

Секретарь. Хороший секретарь все еще будет стоить дешевле, чем компьютер с системой распознавания речи, способной различить слова "да", "два" и "на". Она сможет печатать со скоростью мысли, набирать и отсылать письмо, которое нужно шефу, а не то, которое он диктует, следить за деловыми встречами и юбилеями - а также делать кофе, обдумывая подарок на день рождения жене босса.

Автомеханик. Уже в 1990-х большинство автомобильных диагностических приборов на самом деле представляли собой специализированные компьютеры. Автомеханик с нейро-интерфейсом сможет "попасть внутрь" автомобиля, и, перемещаясь по его схемами и узлам, найти поломку. Со временем это станет еще важнее, поскольку все больше систем обычного автомобиля будут работать под управлением компьютера.

Музыкант. В картине "История Бадди Холли", Бадди говорит: "в моей голове звучит музыка, которую никто никогда не слышал". Используя нужные секвенсоры, дискритезаторы и синтезаторы, музыкант может возродить эту музыку к жизни. Он сможет мысленно управлять получившей к тому времени широкое распространение электронной музыкальной аппаратурой, такой как духовые и клавишные цифровые инструменты. Кроме того, используя цифровые преобразователи, "компьютерный мозг" сможет слушать музыку, направляя ее непосредственно в мозг, минуя уши. Это значит, что люди наконец-то смогут слушать музыку без искажений и с любой громкостью, не беспокоя этим окружающих и не боясь оглохнуть! Это также означает, что через Сеть или локальное подключение музыканты смогут создавать, сводить, выпускать и "слушать" музыку, которую раньше никто не мог услышать - т.н. "закрытый джем-сейшен". Чип с такими записями иногда стоит больших денег.

Писатель. Больше не нужно сидеть за клавиатурой или печатной машинкой, уставившись в пустой экран или на чистую страницу. Нейро-интерфейсы помогут писателю во всем, начиная от исследования первоначальной идеи и заканчивая ее воплощением на бумаге. Интерактивная "помощь писателю" поможет писателю с планом произведения; имитаторы личности смогут предсказывать поведение персонажа при заданных обстоятельствах.
Авиадиспетчер. Просто наблюдая за летной моделью, диспетчер сможет управлять самолетами, используя более сложные схемы, чем это возможно в настоящее время. Он будет видеть трехмерную модель положения самолетов в воздухе и отдавать им команды голосом. Вспомогательные компьютеры будут следить за курсом и топливом самолетов, предупреждая о слишком близком их сближении и других проблемах.

Кибердеки
Кибердека - это вид персонального компьютера. Однако, в отличие от обычных компьютеров, кибердеки предназначены для выполнения специализированных программ - работающих напрямую с мозгом пользователя через нейро-интерфейс. У большинства моделей есть клавиатура для вспомогательного управления, но помните, что главное средство контроля за кибердекой - выключатель питания.
Для достижения максимального быстродействия большинство кибердек запускает программы прямо с ПЗУ-карт (см. стр. 65), а не с диска. Вся информация о быстродействии программ основана на этом. Если программа запускается с диска, удвойте количество Командных этапов, необходимых для ее выполнения.
При выборе кибердеки нужно учесть три фактора: ее Сложность, быстродействие, и количество слотов.
Сложность: У кибердеки, как и у любого другого компьютера, есть своя Сложность. Поскольку большинство программ для нетраннинга имеют Сложность 2, есть существенная разница между кибердекой Сложности 2 (которая может выполнить две программы такой Сложности одновременно) и Сложности 3 (который может одновременно выполнить десять таких программ!). Для увеличения производительности кибердеки нужно несколько специализированных нейро-сопроцессоров. Вместо обычного 50%-ого увеличения стоимости при увеличении производительности на 50%, для кибердек стоимость еще раз удваивается. Таким образом, кибердека Сложности 2, способная выполнять одновременно три программы Сложности 2 вместо двух, будет стоить 50,000$!

Стоимость кибердеки

Сложность	Базовая цена
2	25,000 $
3	250,000 $
4	1,500,000 $

Индекс Быстродействия: Индекс Быстродействия кибердеки (ИБ) показывает, насколько быстро она способна обработать информацию при работе через нейро-интерфейс. ИБ показывает, насколько кибердека быстрее стандартной деки, ИБ которой принимается за единицу. Чем выше ИБ деки, тем она быстрее; Графический интерфейс, запущенный на деке с ИБ 4 займет только 1,000 миллисекунд за этап (четверть обычного времени его выполнения)! Конечно, некоторые деки медленнее (и дешевле); на деке с ИБ 1/2 тот же самый этап займет полных восемь секунд.
ИБ только что купленной, стандартной модели кибердеки принимается за единицу. Увеличение быстродействия стоит денег! За каждую дополнительную единицу ИБ прибавляйте 25% к цене деки (до максимального ИБ 10 при цене на 225% больше). И наоборот, можно немного сэкономить деньги, покупая деку медленнее обычной. За каждых 0.1, вычтенных из ИБ, уменьшите цену деки на 10% (до максимальной скидки в 50% за ИБ 0.5). При вычислении длительности этапа модифицированной деки, округляйте время до ближайших 100 миллисекунд (например, 1250 миллисекунд округляются до 1300, в то время как 1249 миллисекунд - до 1200). Пример: дека Сложности 2 стоит 25,000$. Улучшение ИБ до 3 (в три раза быстрее, чем обычная дека Сложности 2) будет стоить еще 50% (12,500 $), и ее этап будет длиться 2666 миллисекунд (округляем до 2700).
Слоты: Количество слотов определяет, сколько ПЗУ-карт может быть подключено к кибердеке одновременно. Это не значит, что все эти программы или базы данных будут выполнятся одновременно - дека, способная выполнять одновременно только две программы, может иметь слоты для десятка. Переключение с одного слота на другой занимает один этап. Кибердеки выпускаются с двумя встроенными слотами. Каждый дополнительный слот увеличивает ее стоимость на 10%.

Окончательная стоимость
Расчет цены кибердеки начинается с покупки модели соответствующей Сложности (с учетом модификаций производительности); затем следует изменение ИБ и, наконец, дополнительные слоты. Если Мастер требует очки персонажа за аппаратуру, каждые 5,000$ цены стоят 1 очко.
Пример 1: Нейрону нужна хорошая кибердека, но денег у него мало. Он покупает деку Сложности 2 (25,000$) и увеличивает ее производительность на 50 % (ее цена теперь 50,000 $). Решив, что ему нужна быстрая дека, он покупает ИБ 5 (цена увеличивается на 100% и составляет теперь 100,000 $). Наконец, он добавляет три слота (каждый стоит 10% от 100,000 $ - еще 30,000 $). Окончательная стоимость его деки - 130,000 $ (и/или 13 очков, по желанию мастера), и ее Командный этап длится 1,600 миллисекунд при использовании Пространственного интерфейса.
Пример 2: Терминатор, один из "наиболее разыскиваемых" декеров матрицы, работает с исследовательской группой над созданием кибердеки высочайшего класса. Он начинает с деки Сложности 4 (1,500,000$) и улучшает ее производительность на 50% (теперь ее стоимость составляет 3,000,000$). Затем он увеличивает ИБ до 10 (плюс 225%; цена становится равной 9,750,000$). Наконец, он добавляет 20 дополнительных слотов (еще 200%). Окончательная стоимость этого чуда составляет 31,500,000$ при Командном этапе в 200 миллисекунд с использованием Пространственного интерфейса, и отделы производственного шпионажа любой корпорации мира будет стремиться заполучить ее!

Стандартные кибердеки

Деки, подобные кибердеке Терминатора, не могут продаваться в розничной сети. Мастер еще до начала кампании должен определить доступные в продаже модели кибердек. Хорошее правило - ни одна дека со Сложностью больше 3 не может быть приобретена через обычную коммерческую сеть. Это не значит, что таких вообще не существует, просто нетраннеру придется потрудиться, чтобы получить подобную!

Умение работы с кибердекой и быстродействие
Чем лучше нетраннер работает со своей кибердекой, тем быстрее это у него получается. За каждые пять полных очков умения Использование кибердеки Командный этап персонажа уменьшается на 100 миллисекунд. Обратите внимание, что этап не может быть короче 100 миллисекунд (за исключением ИИ).
Боевые рефлексы также уменьшают Командный этап на 100 миллисекунд.

Стандартные модели
Мастеру нужно продумать несколько распространенных фирменных кибердек, подходящих под условия его мира. После этого он может не стесняться ограничивать технологию, доступную персонажам - он не должен позволить толстосумам начать игру с наилучшей аппаратурой! Приключенцам придется попотеть над созданием деки, как у Терминатора, а не просто выложить кучу денег!

Ком-линии
В таблицах создания сети один из вариантов описывает узел, подключенный к ком-линиям (телефонным линиям будущего). Они используются, чтобы позвонить (или получить звонок) на другие компьютеры и связываться с ними через модем.
Ком-линию, позволяющую пользователям узла звонить и соединяться с другими системами, называют ком-линией удаленного доступа (outdial). Она может быть очень полезна, если нетраннер не хочет, чтобы звонок могли отследить (к тому же за него не нужно платить). См. "Фрикинг", стр. 75.

Фрикинг
Осторожному нетраннеру часто будет нужно сделать звонок, который бы казался исходящим не от него. Термин "фрикинг" появился в начале 1970-ых, когда телефонные энтузиасты называли себя "телефонными фриками". Добиться нужного результата можно разными путями:
Переадресация: Самый простой для нетраннера метод - это последовательное подключение к несколькими системам с исходящими линиями. Он будет подключатся с одной системы к другой, пока от настоящей цели его не будет отделять четыре-пять подключений. Настоящий параноик еще и убедится, что все задействованные системы находятся в разных частях мира, или принадлежат различным сетям, что сделает отслеживание практически невозможным.
Этот метод подразумевает наличие у Мастера полной карты сети (или времени на ее создание). Также есть вероятность, что нетраннер случайно подключится к системе, находящейся под наблюдением (скорее всего, по независящим от него причинам), и может быть обвинен в действиях, которых он не совершал!
Пример: Черной Тени (прозвище нетраннера из Небраски, специализирующегося на отслеживании пропавших людей) нужно покопаться в списках лиц, получающих пособие штата Невада. Ему нужен доступ к центральному компьютеру Карсон-Сити, но у него нет на это прав. Он проводит исследование системы и обнаруживает, что она не принадлежит ни к одной из главных сетей; это небольшая правительственная сеть в пределах здания, но к ней ведут пять входящих ком-линий. Он не хочет напрямую подключаться к сети, полагая само собой разумеющимся (и скорее всего, совершенно обоснованно), что все входящие звонки регистрируются и отслеживаются. Однако он знает о компьютере, занятом в мелком бизнесе в Сингапуре, у которого есть удаленная ком-линия. Он включается в сеть и подключается к компьютеру в Сингапуре, чтобы вызвать с него Карсон-Сити.
Чего он не знает - так это того, что дилеры стероидов с черного рынка использовали сингапурский компьютер для отмывания денег, и он находится под неусыпным наблюдением Интерпола. Сразу после его подключения была запущена очень быстрая программа Trace. Следующее, что он узнает - его разыскивает Интерпол для допроса.
Для мастера это отличный сюжетный ход. Он позволяет поддерживать остальной мир в движении и дает игрокам понять, что есть множество вещей, о которых они ничего не знают...
Подключение к коммутатору: Нетраннер, или кто-нибудь из его помощников, знающих электронику, может попросту найти коммутатор ближайшей телефонной компании (большой шкаф, где сходятся все идущие в здание компании провода), подобрать ключи и переключить провода с телефона нетраннера на его соседа (требуется проверка Электроники с +2). Такой вариант по-прежнему очерчивает слишком узкие рамки, но он хотя бы отводит от нетраннера немедленные подозрения - во всяком случае, до тех пор, пока он не попробует проделать такую штуку три-четыре раза на одном и том же коммутаторе...
Портативное подключение: Это похоже на предыдущий вариант, за исключением того, что нетраннер берет с собой деку и вламывается в коммутатор в неком (желательно отдаленном и скрытом) месте. Конечно, всегда существует шанс, что это кто-нибудь заметит!

ИССЛЕДОВАНИЕ КИБЕРПРОСТРАНСТВА

Нетраннер, "включившийся" в деку (через специальный "джек"-разъем, смонтированный в голове - отсюда и термин) начинает со своего "домашнего" узла. Не подключившись к сети, он видит лишь исходящие пути передачи данных (линии связи, радиолинии и т.д.). Подключение к сети осуществляется через Datalink.
После подключения вокруг него появляется отображение сети (точный его вид определяется Пространственными модулями, см. ниже), и он может начинать перемещение. Доступное деке "расстояние" напрямую зависит от ее Сложности. За каждую единицу Сложности нетраннер может видеть один "прыжок". Например, дека Сложности 4 может "видеть" кого-то или что-то в киберпространстве на расстоянии в четыре прыжка (см. ниже "Перемещение в Сети").

Действия
Работа декера в сети состоит из действий, каждое из которых занимает несколько этапов; чем лучше нейро-интерфейс и кибердека, тем они короче. Выполнение нетраннером более одного действия в этап требует броска на Использование кибердеки (см. стр. 26) с пенальти в -3 за каждое действие после первого. Действия включают в себя перемещение с одного узла на другой, выполнение программ, переключение слотов кибердеки, удаленный запуск программ, и поиск в базе данных.
Если компьютерная система выполняет за один этап несколько операций, то к умениям запущенных программ применяется пенальти -3.
Пример: У Джека-Потрошителя умение Использования кибердеки равно 14. Он осматривался около Datex-P, когда заметил за собой Trace (см. стр. 92). Пробуя сделать прыжок отсюда, он одновременно запускает программы Codewall (стр. 93) и Misdirection (стр. 90). Ему нужен результат 14 или меньше, чтобы уйти, 11 или меньше для Codewall, и 8 или меньше для Misdirection.

Перемещение в Сети
Первое, что должен уметь нетраннер - перемещаться в сети с одного узла на другой или в промежуточную точку пространства. Каждое перемещение - это "прыжок". Одним прыжком можно покрыть расстояние до 500 миль (округлять вверх). Таким образом, система в Нью-Йорке будет на расстоянии в пять прыжков (2,000 - 2,500 миль) от Калифорнии. Каждый прыжок занимает один этап. Даже если два узла физически находятся на одной деке, для перемещения между все равно нужен один прыжок.
Спутниковый канал связи (см. "Отображение Сети", стр. 82) позволяет декеру за один прыжок перемещаться на любой канал связи вне зависимости от расстояния до него. Как показано выше, нетраннер Янки может подключиться к нью-йоркскому каналу связи за один прыжок, перейти в Калифорнийский канал за второй, и уйти оттуда в нужную систему Лос-Анджелеса третьим прыжком, потратив на два этапа меньше. Конечно, многие каналы связи защищены от несанкционированного доступа специальными программами...
Спутниковые каналы стоят легальным пользователям 10.00$ за минуту, но многие пользуются ими нелегально.
Если сигнал будет проходить через любую систему, которая, по мнению Мастера, может его замедлить (например, старый механический телефонный коммутатор), он может добавить дополнительные этапы.
Подключение к узлу само по себе обычно не вызывает тревоги (если в системе специально не запущены сторожевые программы для обнаружения и ограничения подключений), и многие системы свободно пропускают через себя сигналы. Для дополнительной информации см. "Отображение Сети" на стр. 82.

Нетраннинг и партия
Для многих сеть является соблазнительным бегством от реальности. И в самом деле, некоторые настолько увлекаются ею, что с большим усилием заставляют себя ненадолго отключиться и позаботиться о своей потребности в пище и воде. Такой персонаж вряд ли захочет физически присоединиться к группе оперативников для вторжения в корпоративную лабораторию - он предпочтет остаться дома и заняться взломом. У мастера может вызвать затруднения необходимость поддерживать баланс между Сетью и реальным миром. Он должен быть уверен, что нетраннеры и остальная часть группы будут достаточно заняты на протяжении всей игры для того, чтобы избежать взаимных упреков в бесполезности. В конце концов, зачем врываться в лабораторию, если нетраннер может проникнуть туда через компьютер и заполучить необходимую информацию? И наоборот, что сможет сделать нетраннер, если цель партии - похищение популярной звезды голографического кино? Эта вопрос подробно обсуждается в Главе 6, но короткий ответ на него таков: Мастер должен убедиться, что некоторые элементы приключения можно разрешить только физически, в то время как другие - только через Сеть.

Что видно?
Область "зрения" декера в сети зависит от его положения. Из случайной точки сети (даже если это не узел) декер может видеть почти все на прямой в пределах С прыжков, где С - Сложность деки. Он будет видеть в пределах досягаемости номер каждого узла и его общедоступный "фасад", который может выглядеть как угодно - от рекламного плаката до огромной запертой двери с надписью "Вон отсюда".
Но даже в пределах С прыжков видно будет не все. Если узел прикрыт программой Camouflage (стр. 93), он, вероятно, не виден. Если узел "сзади" другого, его тоже нельзя увидеть.
(По карте на стр. 94, например, вы должны находиться на узле №106, чтобы увидеть путь к №107, и на узле №107, прежде чем сможете увидеть №108 через №111).

Исследование цели
Первое, что делает нетраннер, когда хочет войти в систему, - изучает ее защиту. Recon (стр. 91) может попробовать найти лед в любой видимой системе в радиусе 1 прыжка. Она также может измерить быстродействие системы по отношению к деке. Mask (см. стр. 93) снижает вероятность успеха этих попыток. Программой Mask можно закрыть определенный или весь лед в системе.
Если в системе запущена Disinformation (см. стр. 93), Мастер должен делать проверку каждый раз, когда Recon не удалась попытка обнаружения льда. Успешный бросок против Disinformation приводит к возврату Recon ложной информации персонажу. Recon также можно применять для подробного исследования отдельных программ (см. стр. 91).
Декер может предпринять только одну попытку изучения отдельной системы. Он может попробовать снова, если улучшит свое оборудование или софт, иначе повторные попытки будут всегда давать тот же самый результат. Исключение: Если со времени последней попытки цель изменила свою систему защиты, мастер должен сделать проверку для каждого изменения с целью определить, обнаружено ли оно.

Вход в систему

Когда декер перемещается на узел ("подключается" к нему), он не может автоматически войти и использовать эту систему - он находится вне ее, перед ее входом. Здесь он получает возможность увидеть лед и другую защиту системы, оценить продолжительность ее этапа, как если бы он запустил программу Recon на уровне своего умения Использования кибердеки. Однако, если только персонаж не скрыт, любой лед увидит его на входе в систему. Тут программы Watchdog или Password обратят внимание на любого. В зависимости от настроек программ, они могут или проигнорировать вроде бы бездействующего гостя, или поднять тревогу.
Чтобы покинуть этот участок и войти в систему, декер должен пройти, легально или нелегально, все установленные программы Password. После этого он в системе. (Но не обязательно в безопасности. Если при прохождении Password была поднята тревога, другой лед может атаковать его в системе или даже после нее!)

Внутри системы
После того, как декер вошел в систему, он может смотреть "сквозь" нее на Сеть. Он также может определить, сколько исходящих линий в системе, являются ли они открытыми (по которым можно перейти куда угодно) или выделенными (которые ведут только к определенной цели). Некоторые исходящие линии будут защищены паролем. Пока декер не преодолеет его любым способом, он не сможет перемещаться или видеть по этим линиям.
В зависимости от уровня доступа, декер также может узнать кое-что о структуре и деятельности данной конкретной системы. Если в системе находятся файлы, он сможет просмотреть хранящуюся там информацию, и так далее. Вся это полностью отдается на откуп мастеру.
Внутри системы для охраны отдельных участков с файлами могут существовать свои программы-пароли, и даже более сложный, чем снаружи, лед. Это рассматривается как полноценная система в системе со своим собственным входом. Но в большинстве систем предполагается, что у любого, прошедшего через главный вход, есть доступ ко всему, что он "видит". Привилегированные пользователи, конечно, видят больше!
Декер с привилегированным доступом может сделать автоматически успешную проверку всего льда в системе с помощью Recon. Он также может остановить или запустить любую отдельную программу, или остановить или запустить весь лед. Каждое "переключение" занимает ход.
Подробнее о возможных действиях декера в захваченной системе см. на стр. 79.

Другие декеры
Декер может увидеть любого нетраннера в пределах своей "области зрения", если тот не скрыт программой Stealth. Обычно другой декер выглядит как размытое пятно или мерцание, пока кто-нибудь не посмотрит прямо на него. Тогда наблюдатель увидит образ нетраннера, назначенный им для своего сетевого двойника, и его скорость. Пока наблюдатель не узнает, кто находится за этим образом, он ничего не может сказать о нем или его действиях. Большинство декеров используют стандартный образ, но при желании его можно менять!

Выполнение программ
В зависимости от денег и качества кибердеки, у нетраннера может быть от одной до нескольких десятков одновременно подключенных ПЗУ-карт. Обычно они не неактивны (оффлайн); количество активных (онлайн) программ зависит от их Сложности и от Сложности кибердеки.
Декер может усилием мысли запустить любую программу с подключенной к деке ПЗУ-карты. Поскольку дека может одновременно запустить конечное число программ, нетраннер при подготовке деки должен назначить им приоритеты, если количество запущенных превысит максимально возможное.
Время выполнения каждой программы включает в себя этап запуска. Таким образом, если декер запускает программу со временем выполнения в один этап, она закончит работу в конце этапа.

К черту единые стандарты!
Одна из проблем совместимости, стоящих перед сетями 90-ых - стандарты интерфейсов. В настоящее время нет единого метода обмена данными - существуют буквально десятки сетевых протоколов.
Большинство сетей в киберпанке описаны с расчетом на то, что из множества стандартов появится один, который и станет единым для всех. Злой (или просто стремящийся к реализму) мастер может не согласиться с этим. Если сети разделены по зонам (все равно, по международным, корпоративным или местным границам), мастер может назначить для каждого участка сети свой протокол связи. Это может вылиться в несколько интересных игровых сессий, когда расстроенный нетраннер обнаружит, что он, как не старайся, не может заставить компьютер из Мексики пообщаться со своей кибердекой. Конечно, у него может возникнуть парочка идей по поиску ПЗУ-карты, которая поможет...

Странные протоколы
Не все компьютеры используют единый протокол связи. Эффективно защитить нужный компьютер можно, изолировав его от сети и сделав так, что любой, кто захочет подключится к нему через обычные ком-линии, должен будет использовать специальное нестандартное "железо" или софт.
Попытки персонажей определить, какие странные программы связи или нестандартные кибердеки нужны для такой работы, могут привести к интересным экспериментам. Например, мастер может подбросить группе кибердеку без имени изготовителя или серийного номера. Кроме загадки ее происхождения выясняется, что она, кажется, не работает ни с одной обычной сетью. Исследуя ее, они со временем узнают, что ее микросхемы были разработаны большой канадской компьютерной компанией.
Во время исследования, группа обнаруживает несколько ком-линий, идущих в комплекс. Подключив к ним обычную кибердеку, они получают бессмысленные данные - но подключив найденную деку, нетраннер оказывается внутри странной сети, подобной которой он никогда не встречал...

СТОЛКНОВЕНИЯ В КИБЕРПРОСТРАНСТВЕ

При попытке взломать компьютер декер в конечном счете столкнется с какими-нибудь защитными программами. Их называют льдом (ICE, Intrusion Countermeasure Electronics - электронное противодействие вторжению). Всегда есть вероятность стычки с враждебным декером, который работает на атакованную систему, или которому нужны те же данные, или просто с недружелюбным сопляком.

Бой
Под "боем" в нетраннинге понимается любая попытка взлома системы или стычка между двумя и более нетраннерами. Обратите внимание, что при одновременном входе в систему нескольких нетраннеров может возникнуть бой каждого с каждым и со льдом, охраняющим систему!

Обезвреживание льда
После применения Recon (стр. 77, 91) для определения параметров льда взломщик может попробовать обезвредить его. Против каждого типа льда есть своя эффективная атака - если у нетраннера нет соответствующей ПЗУ-карты, все атаки рассчитываются по умолчанию (см. стр. 89). Попытка обезвреживания рассматривается как состязание умений между атакующим и льдом.
Если нетраннера настигает критическая неудача при попытке обезвредить лед, немедленно срабатывают все не обезвреженные сигнальные программы. Умный нетраннер обычно начинает с их отключения!

Атака и защита
Как только система предупреждена о наличии взломщика, разница между продолжительностью Командного этапа декера и системы становится очень важной. (Эту же разницу первым делом нужно вычислить в стычке двух нетраннеров). Мастер должен будет отсчитывать время в бою в единицах, равных кратчайшему этапу - если этап Повелителя Деки длится 1,000 миллисекунд, а у атакованной им системы - 500 миллисекунд, мастер должен будет отсчитывать время в интервалах по 500 миллисекунд, так как более быстрая система на каждое действие взломщика будет отвечать двумя.
Программы атаки и защиты выполняются как любые другие - но если нападающий достаточно быстр, защитник может даже не получить возможности ответить! Пример 1: Повелитель Деки (этап длительностью 1,000 миллисекунд) сталкивается с банковским компьютером (этап - 500 миллисекунд) и исследует его с помощью Recon. К сожалению, он терпит критическую неудачу при отключении программы Alarm, и система оповещается о его присутствии.
В первые 500 миллисекунд банковский компьютер одновременно запускает Codewall -14 и Sever -13. Поскольку это два действия за один этап, Sever назначается штраф в -3, так что компьютер бросает против Codewall 14 и Sever 10. К сожалению, у Повелителя не запущено защитных программ, и оби проверки банковского компьютера успешны. Он мельком видит запущенную Codewall, затем испытывает небольшую дезориентацию во время отключения от сети. Сейчас Повелитель Деки сидит в квартире, ошеломленно смотря на пустой экран, и задается вопросом, где бы добыть наличных для покупки деки побыстрее!
Подробности см. в разделе "Атакующие и защитные программы" (стр. 89-92).
Критический успех во время любой атаки нетраннера показывает, что аккаунт, над которым он работает, является привилегированным (см. стр. 69). Если весь лед будет расколот, декер получит привилегированный доступ. В противном случае для достижения такого результата ему придется использовать Promote (стр. 91).

Быстрый взлом
Правила проникновения в систему и сетевых сражений дают существенное преимущество нетраннеру с лучшей аппаратурой. Это может быть неприемлемо для отдельной кампании. Если мастер хочет акцентировать внимание на умениях в противовес оборудованию или упростить расчеты, он может воспользоваться нижеследующими "быстрыми и грубыми" правилами.
Во-первых, используйте состязание умений Использования кибердеки с модификаторами по Сложности вместо всех проверок на атаку и защиту. Во-вторых, замените Командные этапы обычными секундными ходами из GURPS - одно действие в ход и персонаж с наибольшим эффективным умением начинает первым. Наконец, чтобы определить "умение" компьютерной системы (у который нет человека-оператора), умножьте Сложность системы на 4.

Защита от копирования
В мире, где ловкачи-операторы за деньги сделают что угодно, дорогой софт нужно защищать от копирования, или его быстро нелегально растиражируют. Это противоречит тенденциям 1990-х, но соответствует законам жанра.
В любой коммерческой программе будет предусмотрена защита от копирования. Нелегальные копии не будут работать на оборудовании без нужного серийного номера или будут работать не так, как нужно; они могут ввести вирус в систему пользователя или сообщать о краже производителю - все зависит от фантазии мастера.
Поэтому любую скопированную программу перед использованием нужно тщательно проверить на ловушки. Это требует проверки на Программирование, обычно с пенальти -4, и недели времени. Мастер делает проверку втайне. Осторожный пират перепроверит все несколько раз.
Это применимо, главным образом, к программам, скопированным с дисков. Коммерческие ПЗУ-карты почти невозможно скопировать - они обладают дополнительной аппаратной защитой, запаянной в пластик. Аппаратный взлом ПЗУ-карты обычно требует двух недель и проверки на Электронику с -5; неудача означает ее самоуничтожение. Успех означает возможность скопировать программу, хотя ее все равно нужно будет проверять на отсутствие ловушек.
Любой продавец пиратского софта будет уверять покупателя в его чистоте. Если он говорит правду, то, скорее всего, товар уже устарел.

Употребление и злоупотребление

Декер, проникший через защиту системы, может делать все, что доступно обычному пользователю. (Если он "позаимствовал" аккаунт легального пользователя, он также обладает всеми его специальными привилегиями). Если он получил доступ в качестве привилегированного пользователя, он может делать что угодно.
Ниже перечислены действия, которые может предпринять предприимчивый нетраннер (кроме обычного запуска программ).

Создание новых учетных записей
Это может делать только привилегированный пользователь. Введя фиктивные данные в системной файл пользователей, он выбирает, создавать ли обычный или привилегированный аккаунт. У обычных пользователей немного прав, но они не привлекают излишнего внимания, тогда как нового привилегированного пользователя, которому доступно все, могут быстро заметить. Если нетраннер может достигнуть цели с помощью обычного аккаунта, или если он уверен в программе Promote то лучше остановиться на обычном аккаунте.
Декер должен помнить, что все его действия наверняка записываются - и если у него нет надежной программы Erase, ему придется бросить аккаунт после его использования для сколько-нибудь заметных действий.
Каждую неделю есть вероятность обнаружения фальшивого аккаунта текущим системным администрированием. Мастер должен скрытно бросить 3d для каждой подложной записи. Если это публичная система, результат 4 или меньше указывает на обнаружение подлога; для обычной нужно выбросить 6 или меньше, а для защищенной - 8 или меньше. Умножьте эти числа на 2, если это привилегированный аккаунт.
Возможная реакция на фальшивку варьируется от обычного удаления записи до запуска мощных программ Alarm и Trace.

Копирование или загрузка информации
Находясь внутри системы, хакер может захотеть украсть часть софта или информации из базы данных. Учитывая размеры таких программ, их передача даже по волоконно-оптической линии займет немало времени. Для взломщика существует и другой путь - можно скопировать объект так, чтобы в системе он находился в двух экземплярах, причем резервная копия располагалась там, куда можно будет добраться еще раз.
Копирование данных внутри машины осуществляется быстро - 1 Гб/мин. Выгрузка информации в другую машину по сети (например, в кибердеку нетраннера) займет 20 минут за гиг.
Размеры программы зависят от ее Сложности - в среднем программа Сложности 1 занимает 1% от гигабайта. Туда входят все справочные файлы, документация, обучение и все, что необходимо для ее запуска. За каждую единицу Сложности размер программы увеличивается в 10 раз (например, программа Сложности 3 займет 1 гигабайт). Подробная информация о размерах баз данных изложена на стр. 67.
Данные можно таким же образом загрузить в систему - хакеру может понадобится временное место хранения "горячей" информации.

Наблюдение за другими пользователями
Декер может использовать программу Monitor (стр. 91) для отслеживания действий другого пользователя. Успешная проверка Программирования минус Сложность системы позволит ему установить Monitor для получения списка действий конкретного пользователя. После этого нетраннер может отключится от системы и, вернувшись позже, просмотреть файл. Вероятность обнаружения программы такая же, как и для подложного привилегированного аккаунта (см. выше).

Удаленное выполнение
Декеру часто нужно будет выполнить программу на компьютере, с которым он связан - чтобы выключить системы защиты, например, и позволить группе соратников незамеченными войти через дверь. Считая, что он обезвредил программы защиты и обладает аккаунтом, с которого можно запустить нужную программу, запуск или остановка программы займет один этап.
Одна из опасностей удаленного выполнения - возможность того, что при запуске (или остановке) программы включится тревога, которую он до этого не заметил. Для проверки этого варианта используется программа Recon.
Время выполнения удаленной программы различно. Поскольку в большинстве своем они выполняются на обычных компьютерах, 10 минут - вполне оправданное время, хотя мастер может изменять его в зависимости от ситуации.

Поиск в базе данных
После получения доступа к базе данных нетраннер может осуществлять в ней поиск. Это занимает 10 минут на 1 Гб. базы данных (см. стр. 66). Поиск в чипе данных требует лишь 1 минуты на гиг (см. стр. 67).

Перемещение ценностей
С появлением электронных переводов, деньги стали перемещаться по линиям связи, а не в бронированных машинах. Изменяя нужные числа, хороший нетраннер обеспечит себе "легальный" доступ к миллионам долларов наличности, драгоценным металлам, товарам и всему, что используется в торговле.
Внешний вид операции по перемещению ценностей зависит от Пространственного интерфейса (см. стр. 88), но обычно это их "сбор" декером с помощью проверки на Компьютерный взлом, затем "перенос" на другой узел или использование программы Transfer (см. стр. 92). В действительности нетраннер похищает коды маршрутизации и номер валютного счета, после чего стирает их из системы предыдущего владельца. Затем он должен договориться о доставке...

Современное оборудование

В мире киберпанка развитие аппаратного и программного обеспечения идет теми же темпами, что и все остальное. Программы атаки и защиты устаревают и теряют эффективность, потому что лихие парни и специализированные ИИ

постоянно находят в них дефекты и выпускают новые версии. Ваш Codewall может не устоять против нового Icepick, но посмеется над его же версией годичной давности.
Мастер должен назначить дату выпуска для всего применяемого софта. Когда две программы участвуют в состязании умений, более старой программе назначается пенальти, как показано в таблице ниже:

1 месяц:-1
2 месяца:-2
3 месяца:-3
4 месяца:-5
5 месяцев:-7
6 месяцев:-9
7 месяцев: -12
8 месяцев: -15
9 месяцев: -18

Софт старше 9 месяцев попросту бесполезен в мире, где так высоки ставки в борьбе с промышленным шпионажем! (Если мастеру для определенной компании эта таблица кажется слишком строгой, достаточно умножить время на 2 или 3.)
Пример: Confuse, датированная 1-1-20 ("Confuse 010120"), атакует Зеленую Великаншу, защищенную программой Damper, созданной 9-20-19. Она старше Confuse на 4 месяца и получает штраф -3 в состязании умений. Ее эффективное умение равно 9 против умения 12 Confuse 010120.
Имейте в виду, что софт - особенно краденный - может быть устаревшим уже во время покупки. В код любой программы вписана дата, которую ее владелец может легко проверить. Но дату можно подделать! Для ПЗУ-карт дата в коде должна соответствовать дате, вытесненной на пластике; любое несоответствие означает, что что-то нечисто. Обнаружить фальсификацию диска невозможно, если у вас нет другой, подлинной копии программы (может быть, вы только думаете, что она подлинная) для побайтового их сравнения; для этого нужна дека с двумя слотами и час времени. Но если вы подозреваете, что ваш Icepick давно устарел, вы можете легко определить это, смоделировав некую ситуацию для проверки.
С другой стороны, умелый нетраннер может иногда разжиться предварительной версией программы, которая фактически "датирована будущим". Такие программы будут иметь преимущество перед любым продуктом, добытым по легальным каналам - если они работают, конечно! Разработчики софта печально известны оставленными в предварительных версиях вирусами, трассировщиками, и другими сюрпризами - просто на всякий случай. И не забывайте про возможность доброй старой ошибки.

Сисоп-в-коробке (Sysop-In-A-Box)
Это сленговое название программы, имитирующей искусственный интеллект. Она может открыть канал связи с пользователем, чтобы "побеседовать" с ним. Качество имитации зависит от Сложности программы и компьютера, на котором она запущена. Чтобы увидеть, не раскрыт ли обман, каждую минуту проводите состязание IQ пользователя против умения программы; она получает +2 в любой ситуации, где пользователь ожидает увидеть реального человека.
"Сисоп-в-коробке", или СВК, часто применяется в качестве "помощи" для интерактивных услуг. Пока пользователь задает вопросы на заранее известные темы, СВК ни в чем не уступит человеку-оператору, будучи намного терпеливее. Бывает, что лихие программисты настраивают СВК для собственной имитации.
СВК может использоваться для компьютерной защиты - обладая доступом к базе данных с информацией о всех легальных пользователях, он может "задавать вопросы" во время их входа в систему. Обычно все начинается с вопроса типа "Привет Боб, как зовут твою жену?". Если в ответе человека, использующего аккаунт Боба, не позвучит слово "Элиза", он продолжит задавать вопросы, пока не убедится, что "Боб" - взломщик, после чего запустит программы вроде Alarm или Trace.
Для обмана СВК нетраннеру нужно выиграть состязание умений - его IQ против 3 х Сложность компьютера. Нетраннер получает пенальти в -3, если не знает основной информации (имя, адрес, родственники, и т.п.) о человеке, чей аккаунт он использует, +2, если он хорошо их знает (на усмотрение мастера). Искусственный интеллект или компьютерная душа (ghostcomp) с биографической базой данных всегда обманут СВК.
Сисоп-в-коробке стоит 10,000$ за единицу Сложности машины, для которой предназначен, сам он имеет Сложность 3 (2 при запуске на персональном компьютере).

Танцы с телефоном
Один из вариантов в таблицах создания случайных сетей (стр. 82) представляет собой коммерческий компьютер, задействованный в отрасли связи. Привилегированный пользователь может сделать с компьютером телко (телефонной компании) множество интересных вещей. Например:
Информация о клиентах: телефонная компания содержит базу данных, известную как CN/A (имя/адрес клиента), в которой перечислены все владельцы ком-линий. К функциям CN/A можно также получить доступ, умело разговаривая по телефону с применением Социотехники (см. стр. 70). Операторы этих баз не очень опытны - все броски на Заговаривание зубов делаются с +2.
Управление линией: Имея доступ к главному компьютерному коммутатору, хакер может управлять конкретной телефонной линией. Он может изменить номер или перенаправить ее, заставить коммутатор считать ее телефоном-автоматом (забавная, на практически бесполезная шутка), занять линию (все входящие звонки получат сигнал "занято") или добавить к ней пару полезных вещей (ожидание вызова, возможность трехстороннего разговора, определитель номера, и т.д.).
Наблюдение: Через коммутатор можно наблюдать за другой телефонной линией. Для этого необходима скрытая проверка Компьютерного взлома -4. Каждый раз, когда хакер использует эту функцию, мастеру следует бросить 3d. При результате 8 или меньше телефонная компания заметила несанкционированный доступ и удалила аккаунт нарушителя.
Подделка счетов: Нетраннер может взломать бухгалтерский компьютер и внести изменения в телефонные счета. Он может уменьшить счет, удалить подозрительные звонки или добавить звонки к какому-либо счету (чтобы бросить на кого-то подозрение или попросту заставить раскошелиться).

СОЗДАНИЕ СЛУЧАЙНОЙ СЕТИ

Исходным пунктом в сети является т.н. домашний узел. Обычно это некий общественный вход в сеть, хотя нетраннер с аппаратурой посложнее может подключаться сразу к спутнику или использовать установку пакетной радиосвязи. Если мастер еще не спланировал какую-то часть сети, ему, возможно, нужно "быстро и грубо" создать ее случайным образом.

Тип узла (бросок 2d):
2 Бросьте 1d:
    1-4 Сетевой шлюз
    5-6 Спутниковый канал связи
3 Банки данных (+3 к броску безопасности)
4 Банковский/Финансовый (+2 к броску безопасности)
5 Научный
6 Малого бизнеса (-1 к броску безопасности)
7 Крупного бизнеса (бросок 1d)
    1-2 Бухгалтерский (+1 к броску безопасности)
    3-5 Отдела кадров/Административный
    6 Исследований и разработок
8 Среднего бизнеса
9 Коммерческая сеть
10 Правительственный (см. ниже)
11 Частная система (-1 к броску безопасности)
12 Коммутатор/Ком-линии удаленного доступа (см. стр. 85)

Коммерческий (бросок 3d)
3 Военного оборудования/Оружия
4 Медицинский/Фармацевтический
5 Религиозный
6 Программного обеспечения
7 Печатных СМИ
8 Транспортировки
9 Развлечений
10 Розничных продаж
11 Производства
12 Средств сообщения
13 Энергетики
14 Продовольствия/Бакалеи
15 Рекламы/Связей с общественностью
16 Теле- и радиовещания
17 Киберкостюмы/Компьютерное аппаратное обеспечение
18 Преступный

Правительственный (бросок 2d)
2 Судебный
3-6 Законодательный
7-11 Административный
12 Вооруженных сил (+2 к броску безопасности)

Количество ком-линий (бросок 1d)
1 1
2 2
3-4 1d
5 2d
6 3d, сделайте новый бросок, подсчитайте сумму

Системная безопасность (бросок 1d с учетом всех модификаторов за безопасность)
1 Публичный
2-4 Обычный
5 + Защищенный

Обратите внимание, что самые защищенные системы обеспечивают свою безопасность на физическом уровне. В большинстве случаев они вообще не подключены к Сети.

ОТОБРАЖЕНИЕ СЕТИ

Мастеру нужно построить карту компьютерной сети своего мира. Рисовать ее полностью не обязательно (это сотни тысяч узлов), однако иметь подробную карту сети(ей) вокруг "домашнего узла" персонажа необходимо.

Смотря на таблицы создания сети, мастер может заметить, что у множества систем слабая защита или ее вообще нет; они будут публичными или обычными. Так оно и есть. Подавляющее большинство компьютеров будут "обычного" типа, потому что многие сисопы/владельцы не считают, что их система может кого-то заинтересовать.
Мастер должен удостовериться, что наиболее очевидные цели - банковские, коммерческие, военные, исследовательские и т.п. компьютеры соответственно защищены.

Случайные подключения
Чтобы войти в матрицу, декер просто включается в ком-линию и через нее выходит в сеть. После этого он может начать подключаться к случайным узлам. Если мастер хочет подключить его к определенному узлу, пусть так и сделает. В противном случае ему придется создавать произвольный узел (мастер может сделать это заранее, чтобы не тратить времени по ходу игры). Узел представлен в виде пиктограммы. Не у всех систем будет заполнена вся информация - у спутников, например, нет никакой Сложности или Типа. При первом столкновении с системой мастер не должен показывать игроку ничего, кроме Номера узла и Пиктограммы - остальное он должен выяснить сам!

[рисунок стр. 82]

Номер узла: Назначается мастером исключительно для учета (хотя при использовании реалистичной сети можно назначать вместо него какие-либо сетевые адреса).
Пиктограмма: Для каждого типа системы есть своя пиктограмма, которая позволяет мастер или игроку, знакомым с ними, быстро идентифицировать ее. Звездочка указывает на правительственную собственность. Символ бесконечности означает искусственный интеллект.
Сложность системы: Подсказывает мастеру скорость выполнения системой атакующих и защитных программ.
Тип системы: См. стр. 68. Это или *P* (публичная), или *N* (обычная), или *S* (защищенная).
Количество ком-линий: Показывает, сколько пользователей могут подключиться к системе извне. Внутри здания, где она расположена, к системе может быть подключено множество пользователей, но количество внешних входящих линий обычно невелико. У многих систем линии связи настроены на отказ в соединении, если запрос не исходит из строго определенного места; это не лед, а аппаратная функция - ее нельзя изменить. Но посылать внешний запрос такие системы могут.
Когда декер подключается к системе, он занимает одну ком-линию. Оставшиеся можно использовать в качестве исходящих в Сеть ком-линий. Преимущество состоит в том, что такое подключение проследят до этой системы, а не до домашнего узлу нетраннера.
Ком-линии можно использовать для подключений по всему миру. Обычно у них есть встроенный факс и синтезатор/распознаватель речи, так что можно установить обычную связь (у систем Сложности 5 и выше могут быть и синтезаторы голографического изображения, что позволяет подделать видео подключение ...)
Связи системы: Если две системы через сеть непосредственно связаны друг с другом, они подключены к одной линии. Если есть несколько географически близко расположенных систем, они все могут быть подключены к одной и той же линии. Если нетраннер не находит прямого пути от одной системы к другой, ему придется перемещаться через другую машину. У ссылки между двумя системами должно быть число, показывающее количество прыжков между этими двумя узлами. Мастер должен определить и записать тип и способ действия защитных программ в системе. Для примера см. "Запуск программ" на полях стр. 83 и схему сети на стр. 94.

Наездники
Один нетраннер может быть "наездником" для другого при условии их одновременного включения. Один из них просто решает быть наездником; его софт делает все остальное, автоматически перемещая его вместе с партнером, если тот на это согласен и скорость ведомого не меньше. Эти два декера занимают одну и ту же "позицию" в киберпространстве, пока не разделяются. Это значит, что эксперт может везти ученика или помощника через глубокий лед для обучения или помощи в сложной ситуации.
Чтобы "оседлать" ничего не подозревающего противника, нетраннер должен быть в том же самом "месте" и выиграть состязание умений Использования кибердеки, атакующий получает пенальти -8. Продолжительность этапа у атакующего должна быть не больше, чем у жертвы. Если бросок нападающего успешен, он незаметно "седлает" другого декера, и может автоматически следовать за ним. Если проверка провалена, его обнаружили. Новое состязание умений, но без пенальти, назначается каждый раз, когда "лошадь" запускает Recon; декер может внезапно понять, что он не один!
Если в этой области есть другие декеры, они делают проверку без пенальти, чтобы заметить потенциального наездника.
Чтобы "оседлать" не желающего этого противника, нетраннер должен поймать его программой Snare. После этого атакующий должен выиграть состязание умений Использования кибердеки с пенальти -4. Позволяются повторные попытки, но каждая последующая делается с -1. Успех указывает, что декеры теперь в связке. Однако "лошадь" может всегда "сбросить" наездника, отключившись!
В некоторых деках смонтирован разъем "наблюдателя". Любой, кто подключится к нему, сможет "видеть" все, что делает ведущий нетраннер, свободно общаться с ним, но не может предпринимать никаких самостоятельных действий. Такой разъем стоит 1,000$.
Каждый раз, когда два декера находятся в связке или в пределах прямой "видимости" в Сети, они могут свободно общаться. В игровых терминах - игроки могут говорить в реальном времени, хотя мастер не должен разрешать длительных разговоров в горячке сетевого боя.

Искусственный интеллект
Способны ли компьютеры развиться до такой степени, что обретут возможность самостоятельно мыслить? Мастер, водящий киберпанк, должен ответить для себя на этот вопрос. Ниже изложена механика и игровые/социальные последствия введения в мир искусственного интеллекта.

Как это могло произойти?
Случайное возникновение: Поскольку компьютеры делаются все сложнее и сложнее, становится все труднее понимать то, что происходит у них внутри. Обладая гигабайтами оперативной памяти и доступом к базам данных, включающим в себя почти все человеческое знание, научно-исследовательский проект может обезуметь... вирус может развиться в нечто за пределами самых диких мечтаний его создателя... программа, созданная для сбора информации, может сама начать изучать ее. Если это произойдет, узнает ли об этом человечество? Останется ли новорожденная сущность скрываться внутри Сети или явит себя миру? Каковы ее цели? Что ей нужно - мировое господство или просто большее количество памяти? Воспримет ли она существование неэлектронной жизни или будет считать людей помехой, не стоящей внимания?
Намеренное создание: Когда-нибудь ученые-компьютерщики разработают алгоритмы, необходимые для возникновения искусственной "жизни". Но как определить параметры искусственного интеллекта? Можно ли запрограммировать преданность? Если да, то кому - одному человеку, одной корпорации, всему человечеству? Пожертвует ли искусственный интеллект существованием ради защиты того, кому должен быть предан? Если нет, то как далеко простирается его лояльность?
Если существует возможность разработки лояльного ИИ, он будет часто встречаться в корпоративных и в правительственных компьютерных системах. В конце концов, машина может работать 24 часа в сутки - она не заболеет и не будет просить повышения (если правильно запрограммирована, конечно). Она не забывает распоряжений. Короче говоря, она может стать идеальным работником.
Символ бесконечности на пиктограмме системы обозначает искусственный интеллект.

Время разработки и стоимость
Для создания и доводки ИИ, предназначенного для конкретной корпорации, на базе обычного мегакомпа (см. стр. 63), нужно не менее года. В конце года мастер делает бросок 3d. При результате 10 или меньше искусственный интеллект "пробуждается". Если этого не произошло, бросок можно делать по прошествии каждых трех месяцев. Содержание необходимого штата программистов обходится в 750,000$ в год.
Искусственный интеллект всегда является привилегированным пользователем в своей системе. Любой ИИ может перемещаться по сети, если это не запрещено создателями.

Способности искусственного интеллекта
У всех ИИ минимальный IQ равен 15, а каждое дополнительное очко стоит 250,000$, вплоть до максимального значения 22. В дополнение к стандартным программам для ИИ могут быть куплены обычные ментальные умения. Каждое очко персонажа, которое нужно вложить, равняется 20,000$ (т.е. умение на 14 очков персонажа стоит 10,000$; на 16 - 320,000$). Можно купить и физические умения - в таком случае считайте DX равным 12; компьютеру для выполнения большинства физических задач будут нужны соответствующие манипуляторы/дистанционные устройства, стоимость которых остается на усмотрение мастера и обычно составляет 500,000$ +.

Отыгрыш искусственного интеллекта
Возможно, игрок захочет использовать ИИ в качестве персонажа. В таком случае на баланс очков можно не обращать внимания. Мастер должен вместе с игроком создать персонажа, возможно, дав ему 1-3 миллиона долларов. Отыгрыш такого создания - задача для хорошего, опытного игрока, поскольку "всезнающему" персонажу легко оттеснить других персонажей на второй план, лишив игроков удовольствия.

Запуск программ
Точное назначение каждой атакующей или защитной программы определяется мастером. Действительно эффективную систему защиты ему придется "программировать" лично. Например, заметки о существовании в системе программ Watchdog, Trace и Sever недостаточно - мастер (или игрок, если он владелец компьютера), должен определить, как они взаимодействуют. (Да, создание хорошо защищенных систем в киберпанке похоже на создание нашпигованного ловушками подземелья!) Например, мастер может отметить следующее:
Watchdog запущена постоянно и активирует Trace при каждом подключении. Затем она сравнивает полученный от нее результат со списком допустимых узлов, который хранится в файле. Файл может изменять только привилегированный пользователь. При несанкционированном подключении Watchdog запускает Alarm и Sever. Если Sever не выполнила своей задачи, Watchdog начинает удалять важные файлы, пока хакер до них не добрался.
Если программа Recon хакера достаточно хороша, он сможет узнать о Watchdog и отключить ее. Иначе у него будет полно проблем...
Любой, кто знаком с программированием, узнает в этом описании конструкции типа IF (если)... THEN (то) и DO (делать)... WHILE (пока). Если мастер и/или игроки знакомы с программированием, они могут описать защиту системы неким искусственным кодом. На первый взгляд такой метод кажется трудным, но он позволяет достичь любой сложности и делает нетраннинг интеллектуальным соревнованием между игроком и мастером, а не бесконечным бросанием кубиков.
Если мастеру нужна механика взлома проще и удобнее, он может использовать систему на полях стр. 78.

ТИПЫ СИСТЕМ

Научные
Почти в каждом университете, колледже и даже в некоторых средних школах есть компьютерные системы или сети. Тип машин варьируется от персональных компьютеров Сложности 2 до мейнфреймов Сложности 5. В богатых университетах можно обнаружить даже мегакомпы.

В университетских компьютерах обычно развиты сетевые возможности и много входящих и исходящих линий. Зачастую на них также меньше ограничений, чем на большинстве других систем, так что ими часто пользуются для чатов (см. стр. 69), скрытых BBS или распространения самиздата (см. стр. 113).
Взламывать академические компьютеры, если только школа не занята в какой-нибудь современной научно-исследовательской работе, обычно невыгодно. Университетские административные компьютеры зачастую являются хорошим источником информации о бывших (и нынешних) студентах.
У большинства академических систем слабая защита, но у систем, участвующих в важных исследованиях (особенно тех, которые финансирует правительство), будет самый современный лед.

Банковские/Финансовые
Эти системы используются для торговли наличностью, акциями, векселями, ценностями и чем угодно стоящим. Естественно, они должны быть самыми защищенными системами в сети - мастер обязан позаботиться, чтобы финансовые системы в его мире могли взломать только самые лучшие нетраннеры.
Обычно такие системы запускаются на мейнфрейме или мегакомпе, и если ИИ широко распространены, один из них обязательно будет отвечать за защиту больших банковских систем.
Все системные события - каждое подключение, каждая команда - скорее всего регистрируются как в машине, так и на бумаге, так что для успешного взлома, возможно, придется физически посетить узел. Мастер не должен произвольно создавать программы защиты - он должен задать их вручную. В обычной средней системе будет запущена Watchdog, которая запускает Trace и Sever в ответ на несанкционированное подключение, Mask, и множество программ Datalock и Codewall. Зачастую ссылки к банковской системе будут прикрыты программой Camouflage.

Коммутаторы / Ком-линии с удаленным доступом
Чтобы служащие могли соединиться с внешним миром, в некоторых компаниях установлены целые блоки модемов или ком-дек. Они не реализованы в виде отдельной системы, а имеют собственный встроенный софт. К сожалению, у них обычно слабая защита. Большинство таких систем рассматривается как машины Сложности 2 с запущенной Password 12. Бросок по таблице Ком-линий определяет количество исходящих линий; с вероятностью 50/50 любая из них сейчас занята. Для ее освобождения нужно подождать 5d минут.

Правительственные
Существуют тысячи правительственных учреждений, бюро, отделов и агентств, которым нужны вычислительные мощности. Таблица Типов правительственных систем показывает мастеру сферу деятельности конкретной системы, но подробности он определяет лично. Если в данном мире правительства конкурируют с корпорациями, они фактически могут быть корпоративными системами!
Звезда внизу любой пиктограммы указывает на правительственную систему.

Судебные
Судебные системы обычно представляют собой большие базы данных о преступниках и текущих расследованиях. Как правило, они хорошо защищены, а их взлом вызовет большой общественный резонанс (если предположить, что о нем узнают).

Законодательные
Законодательные системы в основном используются законодателями для хранения текущих законов, информации об избирателях и т.п. Одной из самых интересных вещей в законодательной системе может быть список спонсоров предвыборной компании (и возможно, номера счетов, на которых хранятся деньги!)

Административные
Административные системы - это типичные оплоты бюрократизма, большие системы с гигабайтными базами данных по множеству вопросов, начиная от переписи населения и заканчивая распределением осадков. Большая часть правительственных компьютеров будет выполнять административные функции.

Вооруженных Сил
Легкодоступные системы никогда не будут контролировать оружие (такие системы всегда изолированы от сети и не имеют входящих линий)! Скорее всего, они будут заняты всякого рода снабжением и администрированием. Это не значит, что в них не будет стратегически важной информации...
Системы, которые содержат тайную или совершенно секретную информацию почти всегда недоступны из общей сети. Это не значит, что они не сетевые - но к этой сети доступ есть только из некоторых физических мест.
Нетраннеры должны быть внимательны при взломе правительственных компьютеров. Частные компании обычно не будут нервничать из-за кого-то, кто стоил им всего несколько сотен (или даже тысяч) долларов - разыскивать такого взломщика попросту не выгодно. Правительству, с другой стороны, не нужна прибыль - оно охотно бросит большие средства на выслеживание и устранение любого, от кого может исходить даже незначительная угроза.

Крупного бизнеса
Большинство машин в сети принадлежит крупным фирмам и корпорациям. Без больших вычислительных мощностей компании такого размера просто не могут работать.

Бухгалтерские
Используются для повседневного управления активами корпорации. Они обычно хорошо защищены, поскольку часто являются целью как для независимых нетраннеров, желающих быстро подзаработать, так и для промышленного шпионажа. Обычно для таких систем используют микрофреймы, но большие корпорации могут применять и мейнфреймы.

Отдела кадров/Административные системы
Системы такого типа заняты документацией, касающейся служащих - отчеты, личные данные, задания, страховки, отпуска, больничные, и т.д. Для них характерно использование миникомпов или микрофреймов и относительно слабая защита.

Исследований и разработок
Используются учеными для хранения данных и выполнения расчетов. Как правило, это большие и мощные системы, способные обслуживать множество пользователей и быстро выполнять сложные вычисления - мейнфрейм или мегакомп. Степень защиты зависит от конкретной системы. Компания, разрабатывающая новый нервно-паралитический газ, будет иметь защиту мощнее, чем та, что разрабатывает новый клей.

Среднего бизнеса
Эта системы также весьма распространены и используются в офисах средней руки для компьютерного обеспечения деловых операций. Зачастую к ним подключены персональные компьютеры отдельных пользователей со Сложностью 2. У таких систем обычно устаревшая защита и в них мало интересного для сетевого взлома.

Мелкого бизнеса
Чаще всего это миникомп или микрофрейм, который обеспечивает работу всего мелкого бизнеса - инвентаризацию, платежные ведомости, счета и другие записи. Как и выше, на них обычно установлена защита, соответствующая значимости хранимых данных

Сетевой шлюз
Этот узел соединяет вас с другой сетью. Это не столько компьютер, сколько постоянно подключенная к другой сети ком-линия с возможностью удаленного доступа. Адресата этого шлюза может выбрать мастер; это может быть другая сеть, случайно созданная с помощью таблиц. Некоторые шлюзы будут защищены с помощью Password.
В таком случае они трактуются как системы Сложности 2 с программой Password 12, если только сеть не имеет отношения к военной или секретной информации - тогда и умение, и Сложность будут выше.

Частные
Она может быть чем угодно - от персонального компьютера Сложности 2 с модемом до мегакомпа - все зависит от владельца. В общем случае, это маленькая система, защищенная только паролем, без исходящих линий, и не представляющая абсолютно никакого интереса для нетраннера. Хотя мастер волен подойти к этому более творчески...

Спутниковый канал связи
Это подключение к системе спутниковой связи COMSAT (Communications Satellite Corporation - Корпорация Спутников Связи). Отсюда можно напрямую подключиться к любому каналу в мире, что предоставляет практически неограниченную свободу, но увеличивает на один прыжок путь всех данных, проходящих через него.

Коммерческий компьютерный сервис
Существует множество систем, на которых пользователи могут купить машинное время. Современный эквивалент этой услуги- сети вроде CompuServe или GENIE. Пользователи входят под купленным аккаунтом и используют систему для чего угодно - от электронной почты до проведения исследований и бронирования авиабилетов. Для обычного коммерческого сервиса цены составляют от 20.00$ до 60.00$ в час.

Банки данных
Время от времени кому-нибудь требуется безопасное, надежное и полностью анонимное хранилище данных. Банки данных позволяют нетраннеру платно использовать большие объемы защищенного автономного запоминающего устройства. Легально банки данных чаще всего используются для хранения резервных копий. Нелегальное их использование варьируется от хранения украденных программ или баз данных до ведения бухгалтерских книг преступных группировок. В банках данных вся информация обычно зашифрована (см. стр. 63).
Хранение информации в среднем банке данных стоит 1,000$ в неделю за гиг. Лучшие швейцарские аналоги дороже в сотни раз. Оплата обычно производится через анонимные системы электронных платежей, а доступ предоставляется по уникальному коду и паролю. Если кто-то их забудет, то ему не повезло - он может попрощаться со своими данными.

Замóк
Система, предназначенная исключительно для защиты. Замок чаще всего используют в качестве входной системы коммерческих сетей. Обычно это система высокой Сложности, снабженная максимальным количеством слотов и множеством находящихся на дисках программ льда. У большинства из них, кроме обычного льда, всегда запущен какой-либо "сисоп-в-коробке" (см. стр. 80).

И что теперь с этим делать?
Итак, вы только что раскололи большой кусок льда, пробили дорогу сквозь схемы центрального компьютера и нашли данные о партии алмазов. Как их заполучить физически?
Чаще всего при взломе компьютера с целью похитить ценности вам нужно помнить, что деньги, информация, ценные бумаги вроде акций и векселей - это на самом деле лишь биты данных, хранящиеся в памяти компьютера. Изменив пару бит, вы можете легко изменить "адрес" информации, позднее перенаправив ее на один из ваших легальных аккаунтов.

Но что делать, если информация представляет собой физический товар, который не переместишь изменением битов в компьютере? Давайте вернемся к примеру с алмазами. В этом случае "адрес" данных, упомянутый выше - это грузовая декларация, которая просто определяет, чья это собственность. Хитрый декер изменит адрес, направив алмазы прямо к перекупщику, который продаст их за небольшой процент со сделки. В сложных или необычных ситуациях декер может направить их по адресу, который он контролирует (к себе домой, например), но это значительно увеличивает вероятность того, что операцию отследят.

Козырные карты

Иногда нетраннеру будут попадаться ПЗУ-карты, созданные для взлома одной определенной системы. На них часто находится несколько модифицированных атакующих программ. Такая карта называется "козырной".

Она предназначена для одной компьютерной системы и бесполезна для всех остальных. Однако с ней она работает вдвое быстрее обычной ПЗУ-карты и получает +2 ко всем проверкам. "Козырная" карта уничтожается после одной попытки, как успешной так и нет.

Микрочипы, из которых она состоит, почти всегда запаяны в практически непроницаемый пластик. Любому, кто попытается его вскрыть и скопировать программу, нужен критический успех при проверке умения Электротехники; неудача разрушит чип.

Сигналы опасности

Одной из особенностей кибердек является способность уведомлять нетраннера о грозящей опасности и ее происхождении. С текстовым или графическим интерфейсом это не проблема. Характер угрозы объясняется на экране текстом ("ВНИМАНИЕ! ОБНАРУЖЕН ЛЕД. ЭТОТ КОМПЬЮТЕР ИСПОЛЬЗУЕТ FLATLINE. ВЕРОЯТНОСТЬ УНИЧТОЖЕНИЯ ЛЬДА 36%. РЕКОМЕНДОВАНО НЕМЕДЛЕННОЕ ОТКЛЮЧЕНИЕ") или узнаваемой пиктограммой (с заранее заданными уровнями опасности, от маленького ребенка с рогаткой или Большого Серого Волка до чудовища из японских фильмов).

В пространственных интерфейсах предупреждения вообще могут воплощаться в объекты и людей по желанию пользователя. При настройках типа гангстерских 1930-ых, например, защитная программа может предстать в виде конкурирующего бандита, причем его оружие покажет тип угрозы. При настройках в форме абстрактного искусства, персонаж мог бы задать для опасности один цвет (обычно красный). Яркость цвета укажет на степень угрозы - от очень тусклого до яркого и мерцающего. (Это объясняет, почему декеры зачастую долго работают только с одним определенным типом интерфейса - они учатся распознавать сигналы опасности этого "мира"). Однако часто будет попадаться информация, которую система не сможет изобразить из-за отсутствия нужных настроек или из-за необходимости сообщить декеру подробности. Такая задача чаще всего решается аудиосредствами. В гангстерских настройках может подойти помощник и прошептать нужные данные на ухо персонажу; в интерфейсе в виде истребителя второй мировой информация поступает по радио в кабину, когда на горизонте появляется вражеский "Зеро".

Мусор человека...

Собирая информацию о человеке или компании, много времени обычно уделяют скрытому наблюдению с помощью дорогостоящей аппаратуры, записывая каждое движение и слово. Погрузившись в эти шпионские игры, наблюдатели зачастую пропускают один из лучших источников информации - мусор.

Существует множество полезной (и не очень) информации, которой можно выудить из мусорного ведра. Люди, которые и в мыслях не допускают важных разговоров по домашнему телефону, опасаясь прослушивания, способны бегло набросать подробную (а иногда и компрометирующую) информацию на клочке бумаги, который позже выбросят вместе с кожурой от апельсина - иногда предварительно порвав бумагу, но не так, чтобы ее нельзя было восстановить.

Современные хакеры используют эту методику для сбора информации о телефонных и компьютерных компаниях - они называют это мусоросборкой. Легальные пользователи (особенно низкооплачиваемые служащие вроде операторов ввода данных) часто записывают свои аккаунты и пароли на случайных бумажках, которые позже попадают в мусор. Одна из крупных телефонных компаний повесила в офисах плакаты, призывающие служащих "все уничтожать". Как же, так они и сделают! Даже если хакеры не находят собственно аккаунтов, они могут найти распечатки компьютерных сессий, которые покажут правильный формат использования команд - неоценимая помощь для некоторых сложных операционных систем. (В игровых терминах это означает бонус от +1 до +3 к умению Компьютерный взлом для данной системы). Другая полезная информация, которую можно обнаружить в мусорном ведре - это информация о кредитных картах (если персонаж роется в мусоре крупного розничного магазина или компании товары-почтой), номерах телефонов, торговых чеках и другие бумажки, которые можно использовать при заполнении базы данных на человека.

Могут выбросить даже целые диски; в зависимости от профессионализма пользователя, данные с них могут быть стерты, тщательно или небрежно, или не стерты вообще. Удаление всех файлов не уничтожает диск; программы "восстановления" распространены и эффективны даже в 1990-ых. Чтобы прочитать очищенный диск или другие носители, сделайте проверку на Использование компьютера с -2. Мастер может изменять этот модификатор для осторожного или небрежного пользователя.

А если объект наблюдения производит аппаратные средства, в мусор могут попасть работающие микросхемы памяти, ПЗУ и кто его знает, что еще...

Как заполучить мусор? Это зависит от физической защиты помещения. Если персонажи хотят порыться в мусоре из чьего-то дома или квартиры, то это обычно сводится к обнаружения и вывозу отходов до того, как это сделает мусорщик. Хотя здания множества компаний ограждены, иногда (9 или меньше на 3d6) у них есть контейнеры снаружи на случай переполнения.

Если ящик с мусором огражден, но находится снаружи, для доступа к нему может потребоваться пара кусачек и успешная проверка на Скрытность. Метод попроще заключается в изображении команды мусорщиков и обычном сборе отходов. В конце концов, кто станет притворяться мусорщиком?

Если персонажам нужен мусор из конкретного офиса, они могут наняться (или притвориться) швейцаром в нужное здание. Это может занять одну-две недели, но вполне окупиться за счет получения необходимого доступа. Другая распространенная хитрость, используемая людьми, подходящими по возрасту для средней школы или колледжа, заключается в связи с фирмой по поводу школьной кампании сбора макулатуры. Большинство больших компаний очень заботится о своей репутации и с радостью примет участие в таком достойном мероприятии. Если уж *очень* заботиться о прикрытии, то можно организовать настоящую кампанию по сбору макулатуры и даже сдавать ее, но только предварительно просмотрев нужные бумаги!
Сбор мусора с хорошо защищенного участка сам по себе будет целым приключением.

Самозащита
Мастер не должен забывать, что эти же методы могут использоваться против персонажей. Партия, которая обязательно сжигает записки, стирает файлы и ломает диски, осторожно относиться к историям, связанным с мусорщиками, с меньшей вероятностью подвергнется атаке собственных систем.

Компьютерная периферия
Принтер: Подключенный к любому компьютеру, принтер может распечатывать текст или цветные изображения с фотографическим качеством. Он питается от компьютера, весит четыре фунта и стоит 100$. Сто листов бумаги или пластика для печати весят 1/2 фунта и стоят 1$.
Сканер: Это - светочувствительное устройство, способное считать документ или картинку (10" x 15" или меньше) в память компьютера в качестве графического изображения или текста. Он складывается для хранения в однодюймовый куб и питается от компьютера.
Стоимость - 40$, вес - 2 фунта.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КИБЕРДЕК

У софта для кибердек, как и у обычных программ, есть своя Сложность, но, кроме того, для каждой программы задано время выполнения, указанное в этапах. Таким образом, программа со временем выполнения 3 требует для запуска трех этапов. Реальная протяженность этапа по времени определяется типом нейро-интерфейса и Индексом быстродействия кибердеки.
Пример: У кибердеки Сложности 3 этап занимает 4,000 миллисекунд. Если бы ее ИБ был равен 5, этап сократился бы до 800 миллисекунд. Работа с Графическим интерфейсом увеличит этап до 1,600 миллисекунд. Так что выполнение Crash (время выполнения 4) на указанной конфигурации займет 6.4 секунды (1,600 миллисекунд x 4).
У некоторого софта вроде Пространственных модулей, нет неизменного Времени выполнения. В этом случае оно не приводится.

Пространственные модули
В большинстве миров поток данных из нейро-интерфейса поступает по стандартному протоколу (см. поля на стр. 77). Кибердека передает эту информацию программе Datalink (запущенной в деке или встроенной в нейро-интерфейс), которая превращает ее в визуальные образы. Мастер должен решить, доступно ли для каждого пользователя лишь "стандартное" представление киберпространства или каждый может (с помощью соответствующего софта) интерпретировать его по-своему.
Пространственный модуль (ПМ) представляет поток данных из сети в определенном виде, обычно связанном с заданной темой. ПМ разрабатываются с ограниченной возможностью к самопрограммированию, что позволяет им подстраиваться под нужды конкретного пользователя.
В течение некоторого времени ПМ приобретает некую индивидуальность, "изучая", какие программы нетраннер использует в конкретной ситуации, и, возможно, даже давая советы время от времени. После постоянного использования персонажем одного ПМ (не менее двух раз в неделю) в течение трех месяцев, мастер может скрытно бросить 3d, когда персонаж, по его мнению, нуждается в подсказке. При результате 6 или меньше, ПМ даст совет, который может помочь декеру. При 17 или 18 совет будет плохим!
Мастер должен использовать воображение при описании сети игроку. Если персонаж использует Пространственный интерфейс "Космическая одиссея" (см. ниже), мастер не должен просто говорить "Итак, прямо по курсу - компьютер." Вместо этого он, возможно, сумеет описать легко вооруженное торговое судно с позолоченным корпусом! (Конечно, мастер должен назвать игроку любую программу, если игрок потребует). Зачастую время, проводимое в матрице, будет для нетраннера единственным доступным действием во время игры, так что мастеру нужно сделать его захватывающим.
ПМ показывает окружающую среду по-своему для каждого декера. Поэтому один персонаж может видеть схватку в виде магического поединка с летящим в его сторону огненным шаром, в то время как его противник радуется удачному пушечному выстрелу по кораблю конкурента! Ситуация, когда два персонажа встречаются в Сети, требует от мастер скорости - нелегко описывать одно и то же двум людям в разных пространствах.
ПМ стоит 5,000$ и обладает Сложностью 2. Некоторые из самых популярных ПМ описаны ниже.

Космическая одиссея
Нетраннер включается и оказывается на капитанском мостике огромного космического корабля. Киберпространство представлено вакуумом между планетами. Узлы Сети изображены как спутники, планеты и солнца - чем больше поток данных через узел, тем больше звездный объект. Связи между системами представлены маршрутами на гиперпространственной карте. Атакующие программы показаны в виде истребителей или орудий корабля, стреляющих по цели. Защитные программы представлены враждебными истребителями и планетарными силами защиты. Black Ice (см. стр. 93) изображается в виде черной дыры, затягивающей все вокруг... ПМ обращается к пользователю от лица бортового компьютера. Данные представлены в виде высоких исписанных рунами монолитов, которые стоят на поверхности планет. После подавления обороны для поиска нужной информации высылаются

разведывательные зонды. Деньги и товары изображаются в виде астероидов из драгоценных металлов, вращающихся вокруг планеты - с помощью судна их можно захватить и перевезти на другие "планеты".

Пикассо
Это очень стилизованное представление Сети, полное цветных стен и ярких огней. Нетраннер представлен светящийся шаром определенного цвета - чем лучше его аппаратура, тем ярче и больше шар (хотя некоторые декеры предпочитают, чтобы их недооценивали, и намеренно затемняют ауру).
Узлы изображены в виде цветных геометрических фигур - узлы со слабым трафиком одноцветные, а самые популярные - огромные, разноцветные многогранники. Связи между узлами (если они не прикрыты программой Camouflage) видны в виде светящихся неоновых лент - чем они шире, тем больше связей. Данные представлены маленькими кубами с готическими буквами, указывающими на их содержание - товары показываются мерцающими сферами из драгоценных металлов с размерами, соответствующими их стоимости. Атакующие программы представлены сверкающими вспышками лазерного огня, а защитные - сплошными стенами из хрома, кварца или цветного огня. ПМ - маленькая светящаяся пирамида, сопровождающая декера в сети.

Ретро-рок
Этот интерфейс особенно привлекателен для нетраннеров с музыкальными наклонностями и эксцентричным вкусом. Декер играет роль певца/гитариста рок-группы. Каждая программа представлена отдельной песней, и чем громче звук, тем лучше программа и дека. Узлы киберпространства представлены в виде клубов и концертных площадок. Защитные программы - это враждебные толпы людей или вышибалы в дверях - их нужно подавить звуком из усилителя нетраннера (чем лучше атакующие программы, тем громче звук). Данные изображены в виде поклонниц, которые шепчут ему на ухо сладкие биты информации, а товары - это плата за вход. ПМ - менеджер нетраннера, который иногда советует песню, которая подходит, чтобы "завоевать" толпу.

Опасный замок
Один из самых популярных ПМ, Опасный замок предлагает нетраннеру роль средневекового рыцаря, путешествующего через наполненный монстрами замок. Каждая комната - это узел, а коридоры между ними представляют собой связи. Связи под прикрытием Camouflage показаны в виде потайных дверей, а программы защиты - в виде монстров. Легкая защита, например Password (см. стр. 93), представлена маленькими, слабыми монстрами вроде орков, в то время как Black Ice может появиться в виде огнедышащего дракона или мечущего заклинания демона! Атакующие программы - это оружие рыцаря, от кинжалов до громадных топоров и двуручных мечей. Данные представлены в вид набора свитков, а ценности - золота, драгоценных камней и сокровищ. ПМ - это оруженосец, хранящий оружие и сокровища рыцаря.

Другие Пространственные модули
Выше перечислены далеко не все ПМ; еще можно назвать такие модули, как шпионаж (маска и плащ прилагаются), война (управление армией в сражении), магия (могущественный волшебник с множеством заклинаний), сафари (охотник на животных в джунглях), пиратство (плавание по морям данных и захват груженных сокровищами галеонов), мехи (гигантский человекоподобный робот), порнография (это оставляем вашему воображению), и многие другие. Мастер может разработать любой другой ПМ, который он хочет сделать доступным в качестве стандартной программы.

АТАКУЮЩИЕ И ЗАЩИТНЫЕ ПРОГРАММЫ

Все атакующие программы имеют базовое умение 12. Этот уровень может быть изменен обычным путем (см. стр. 65). В некоторых мирах владение этими программами считается преступлением, а в других они доступны в открытой продаже! Если атакующие программы вне закона, мастер должен как минимум удвоить их стоимость, чтобы показать их труднодоступность. Вынудить нетраннеров иметь дело с черным рынком каждый раз, когда им нужно обновление софта - хороший способ занять персонажей и заставить похудеть их банковские счета!
Многие из этих программ разработаны для определенного типа льда - такие программы называют ледорубами.
Большинство программ - как для атаки, так и для защиты - имеют некое значение по умолчанию. Это позволяет персонажу работать с ними без подготовки - *но доступно только для декера с Пространственным интерфейсом*! Ни Текстовый, ни Графический интерфейсы не предоставляют нетраннеру достаточно информации, чтобы за столь короткое время начать атаку или защиту без подготовки. Максимальный уровень по умолчанию - 13, с программами получше просто нельзя работать без подготовки! Обратите внимание, что Компьютерный взлом по умолчанию равен Программированию -4 - уровень по умолчанию можно рассчитать исходя из этого, обычный запрет на "двойные значения по умолчанию" здесь не применяется.
Пример: Инфомаг изучает компьютер, принадлежащий иностранному правительству, и обнаруживает электронную почту, которая ждет доставки в его страну. Она содержит заказ на убийство видного политического деятеля. Маг не уверен в своей способности удалить или перенаправить по неправильному адресу почту, не оставив за собой следов. Он решает, что единственное, что можно сделать - устроить сбой системы, что даст ему время (возможно, анонимно) инициировать правительственное расследование, прежде чем опасное письмо прочитают или удалят. У него нет программы Crash, так что он делает бросок против Компьютерного взлома -4, чтобы вызвать сбой в системе.

Повторные попытки
Обратите внимание на то, что большинство систем глупы. Например, если защита не находится под наблюдением Regenerate, декер может атаковать программой Corrode одни и те же Watchdog или Alarm без пенальти за неудачу. При атаке других программ с каждой последующей попыткой будут накапливаться пенальти. Но большинство программ не понимают, что они атакованы, если они не контролируются другой программой, отыскивающей повреждения.

Bloodhound
Компьютерный взлом -6
Используется для нейтрализации Misdirection. Обычно вызывается программой Trace, если она (или декер) обнаруживает, что потеряла след. Проведите состязание умений между Bloodhound и Misdirection - если Bloodhound победит, Trace сможет продолжить свою работу. В противном случае попытайтесь снова, но каждая последующая попытка идет с накапливаемым пенальти -3, поскольку след "размывается". Время выполнения 1, Сложность 2, стоимость 7,500$.

Confuse
Нет значения по умолчанию
Программа посылает импульс статического электричества по ком-линии. Это не влияет на машины, но декер должен выполнить проверку IQ или будет ошеломлен на 1d секунд из-за сенсорной перегрузки. Если у пользователя есть Fuse (см. стр. 90), программа Confuse должна выиграть состязание умений, прежде чем повлиять на жертву. Время выполнения 1, Сложность 2, стоимость 10,000$.

Corrode
Компьютерный взлом -4
Corrode медленно нарушает целостность программы, давая декеру время удалиться на безопасное состояние от гибнущей системы. После запуска Corrode устройте состязание умений между ней и атакуемой программой. Если выигрывает программа - работа Corrode не приносит результатов. В противном случае программа начинает разрушаться и завершит работу через 1d секунды (предполагается, что это не замечено программой Regenerate). Время 1, Сложность 2, стоит 12,500$.

Crash
Компьютерный взлом -4
За исключением разрушения "железа", Crash - самое страшное повреждение, которая может быть нанесено системе. Как ни странно, Crash одновременно одна из самых простых и доступных программ - но она может быть запущена только с привилегированного аккаунта. Каждый раз, когда Crash запускается в системе с Safety Net (см. стр. 93), немедленно проведите состязание умений между ними или сделайте проверку против умения Crash с пенальти, равным Сложности системы.
Если программа Crash выиграла, атакуемая система немедленно прекращает работу. Все пользователи отключаются, а любые линии, проходящие через нее, считаются подверженными успешному действию программы Sever (стр. 91). Если Crash проваливает бросок, последующие попытки совершаются с накапливающимся пенальти -5 вместо обычного -3 (если она не сработала в первый раз, она вряд ли вообще сработает на этой системе). Время выполнения 4, Сложность 2, и стоимость 15,000$.

Crumble
Компьютерный взлом -4
Используется для нейтрализации Codewall (см. стр. 93). Проведите состязание умений с Codewall - если Crumble выиграет, Codewall будет разрушена. Повторные попытки позволяются с обычными -3. Время выполнения 1, Сложность 2, и стоимость 5,000$.

Disguise
Компьютерный взлом -4
Программа используется, чтобы изменить "внешний вид" сигнала нетраннера, сделав его похожим на легального пользователя узла. Это не даст вам доступ к нему, но обманет любую защищающую узел программу Watchdog (см. стр. 93). Устройте состязание умений между Watchdog и Disguise, чтобы определить, принято ли это подключение за легальное.
Disguise нужна информация о конкретной системе для настройки на нее. Сколько именно ее нужно, решает мастер. Если "настройку" нужно сделать в Сети, декер должно совершить успешную проверку с помощью Recon программы Watchdog, которую нужно обмануть, а затем сделать проверку на Компьютерный взлом -1: это займет 2 этапа. Одна Disguise может обмануть любое количество программ Watchdog, если будет заранее снабжена нужными данными.
Время выполнения Disguise составляет 1, но она должна быть запущена до подключения к узлу, на котором нужно обмануть Watchdog. Ее Сложность 2, стоимость 2,000$.

Erase
Компьютерный взлом -4
У большинства систем существует какой-либо журнал регистрации посетителей системы, их действий и времени пребывания. Особо параноидные системы по мере заполнения печатают эти журналы на бумаге; с этим ничего нельзя поделать, кроме отправки ударной группы в машинный зал для уничтожения доказательств! Однако большинство систем довольствуется находящимся на диске журналом входа и выхода.
Erase используется для уничтожения доказательств одного входа в систему, поиска в базе данных или выполнения программы. Мастер выполняет проверку и не сообщает персонажу результата! (Неудачная проверка означает, что взломщик заблуждается, будто удалил все "следы" - некоторые из них остались). Только при критических успехе или неудаче хакер будет точно знать результат работы программы.
Из умения Erase вычитается Сложность компьютера. Время выполнения 1, Сложность 2, стоимость 8,000$.

Flatline
Нет значения по умолчанию

Этого куска кода в сети бояться больше всего. По сети гуляет бессчетное число ужасных рассказов о нетраннерах, столкнувшимися с "не той" системой или декером - обычно эти рассказы заканчиваются описанием того, как глаза жертвы взрываются от температуры закипевшего мозга.
Эта программа в основном используется крупными компьютерными системами - большинство кибердек недостаточно мощны для работы Flatline, даже если они ее где-то найдут. Она разработана, чтобы отключать хакеров - навечно. Есть множество разных способов убить подключенного нетраннера. Самый распространенный метод (благодаря которому и возникло ее название) заключается в остановке сердца взломщика. Другие варианты основаны на всплеске напряжения, пущенном через кибердеку противника прямо в нейро-интерфейс. Любой из них немедленно причиняет жертве 3d повреждений за каждый этап (PD и DR не защищают) компьютера, на котором запущен Flatline (при условии, что проверка умения прошла успешно, причем она выполняется каждый этап).
Некоторые из более экзотических ее вариантов вообще не убивают. Один из них повреждает нейроны в мозгу, награждая нетраннера недостатком Эпилепсия (хакер может даже не сразу понять это!). Другой гипнотически перепрограммирывает нетраннера, записывая поверх его личности компьютерную душу (см. стр. 56). Оба метода требуют, чтобы Flatline сработала три раза подряд перед отключением - после этого нетраннер не сможет отключиться без разрешения программы. Единственной защитой от нее, кроме отключения нейро-интерфейса, является Fuse (см. ниже). Отключение нейро-интерфейса занимает одну секунду, но быстродействующая система с этапом в 200 миллисекунд будет способна послать за эту секунду пять импульсов - это достаточно, чтобы поджарить большинство нетраннеров до хрустящей корочки.
Мастер должен использовать воображение при создании новых образцов Flatline! Эти программы почти всегда запрещены, и большинство ПЗУ-карт с ними уничтожаются после ограниченного числа использований. Время выполнения 1, Сложность 4, стоимость 1,000,000$+; класс законности 1.

Fuse
Нет значения по умолчанию
Лишь немногие параноики-нетраннеры используют Fuse. Эта программа работает на фоне, пока не обнаруживает нечто похожее на Flatline, проникающую через нейро-интерфейс. Тогда она немедленно отключает пользователя от сети. Fuse может сохранить нетраннеру жизнь, но у нее есть свои недостатки. Во-первых, некоторые программы (включая современный лед) иногда посылают в начале передачи безвредный сигнал, замаскированный под Flatline (см. Bluff, стр. 93). Этот сигнал может быть отфильтрован, если Recon (или нетраннер) распознает, что он ложен, но от него срабатывают многие программы Fuse. Во-вторых, внезапное отключение от нейро-интерфейса дезориентирует и ошеломляет декера на 3d секунд. И, в-третьих, на это тратится ценный слот деки.
Если Fuse запущена, проводите быстрое состязание умений при каждом появлении Flatline (или соответствующей программы Bluff). Если Fuse выигрывает, она немедленно отключает от системы пользователя, не давая нанести ему вреда. В противном случае, за каждую единицу, на которую проиграно, состязание Fuse задерживается на один этап. Критическая неудача означает, что пользователь получит полные повреждения (и, вероятно, мучительно умрет). Время выполнения 1, Сложность 2, стоимость 20,000$.

Icepick
Нет значения по умолчанию
Это универсальная атакующая программа. Она может заменять любую из программ, атакующих лед (Bloodhound, Corrode, Crumble, Disguise, Silence, Skeleton Key II и Webster). Icepick - это выбор опытного декера. Для его запуска нужна дорогая аппаратура. Время выполнения 2, Сложность 4, стоимость 250,000$.

Loop
Программирование -2
Используется для занятия вычислительных мощностей компьютера с целью сделать его менее устойчивым к другим атакам. Обычно программы Loop занимают процессор каким-нибудь бесконечным циклом - вычислением числа Пи, например. При удаче она уменьшает все умения жертвы на 2. Единственная защита против Loop - программа Bailout (стр. 92). Время выполнения 1, Сложность 2, стоимость 4,000$.

Misdirection
Компьютерный взлом -4
Эта программа используется, чтобы сбить со следа Trace (см. стр. 92). Если у преследователя нет Bloodhound (см. стр. 90), он не может продолжать отслеживать путь декера, запутанный Misdirection. Время выполнения и Сложность 2; стоимость 17,500$.

Monitor
Программирование -3
Эта программа используется, когда хакер находится в системе. Если у него привилегированный доступ, он может отслеживать действия любого пользователя этой системы, сделав проверку против Monitor. Время выполнения и Сложность 2, стоимость 25,000$.

Promote
Компьютерный взлом -4
Эта программа запускается с обычного пользовательского аккаунта в системе. При удаче он "повышается" до привилегированного. К проверке против Promote применяется пенальти, равное Сложности системы - чем лучше операционная система, тем сложнее пользователю проделать такую штуку! Время выполнения и Сложность 2, стоимость 20,000$. Эти программы часто попадаются на "козырных" картах (см. поля стр. 84).

Recon

Компьютерный взлом -3
Эта программа используется для исследования системы на наличие защиты - как льда, так и "контратакующих" программ вроде Snare. Когда нетраннер первые сталкивается с системой, мастер должен провести проверку Recon для каждого льда, защищающего узел. Успех позволяет декеру "увидеть" его. Если у нетраннера нет программы Recon, мастер должен делать проверки против Компьютерного взлома -3 для каждого льда, чтобы понять, видит ли его персонаж.
Если в системе запущена Disinformation (см. стр. 93), мастер должен проводить проверку на нее каждый раз, когда Recon провалит свою проверку. В случае успеха Recon выдаст персонажу ложную информацию. Recon также делает проверку на каждой программе Bluff (см. стр. 93) - в случае успеха обман раскрывается.
Декер может также использовать Recon для получения подробной информации о конкретной программе после ее обнаружения. Проведите состязание умений между двумя программами. В случае успеха декер узнает, при каких обстоятельствах исследуемая программа запускается, что и когда может быть ею запущено. При неудаче он не узнает ничего нового. Критическая неудача приводит в действие Alarm, если такая программа имеется. Критическая удача со стороны мастера (который делает проверку тайно), позволяет ему солгать.
Время выполнения 1, Сложность 2, стоимость 7,500$.

Sever
Компьютерный взлом -6
Программа отрезает нетраннера от сети, временно отключая линии связи. Создаваемое нейро-интерфейсом изображение постоянно обновляется из входящего потока данных деки. Если этот поток прерывается даже на доли секунды, изображение исчезает и декер отключается.
Если у жертвы не запущен Shield (см. стр. 93), единственное, что нужно для его отключения - проверка умения.
(Если его кибердека окажется достаточно быстрой, он успеет увидеть начало запуска Sever в первом этапе, и сможет запустить Shield во втором, так как время выполнения Shield равно единице, а Sever - двум). Если Shield запущен, проведите состязание умений между программами. Если Sever проигрывает, дальнейшие попытки атаковать выполняются с обычным пенальти -3.
Время выполнения 2, Сложность 2, стоит 15,000$.

Silence
Компьютерный взлом -4
Используется для подавления любых программ Alarm, запущенных на атакуемой системе. Для каждой из них проводится быстрое состязание умений. Критический успех Silence устраняет Alarm без "видимых" повреждений. Критическая неудача активирует ее! Время выполнения 1, Сложность 2, стоимость 10,000$.

Shield
Использование кибердеки -5
Используется для защиты от Sever (дополнительная информация на стр. 91). Время выполнения 1, Сложность 2, стоимость 12,000$.

Snare
Компьютерный взлом -5
Используется, чтобы ненадолго удержать нетраннера на одном месте. Snare запускается на месте пребывания декера. Она не сможет преследовать декера, если он уйдет с узла раньше, чем программа сработает. Но если он еще на этом узле, то для продолжения движения ему необходимо будет выиграть быстрое состязание умений - Компьютерный взлом против Snare. На каждом этапе после первого жертва может снова попробовать вырваться на свободу с накапливающимся бонусом +1 к проверке (Snare постепенно рушится). Она не мешает использовать программы и не лишает возможности отключиться.
Время выполнения 1, Сложность 2, стоимость 12,500$.

Stealth
Использование кибердеки -5
Хакеры используют программу Stealth, чтобы остаться незамеченными во время перемещения по сети. Чтобы видеть другого нетраннера, обычно не требуется никакой проверки. Однако если у него запущена Stealth, его можно заметить, только когда он окажется на одном узле или в одной точке с наблюдателем. Тогда мастер скрытно проводит быстрое состязание - Использование кибердеки -3 против Stealth.
Каждое удвоение цены отнимает дополнительные -1 из умения Использование кибердеки до максимального пенальти -9. Сложность 2, время выполнения 1, стоимость 10,000$.

Success
Компьютерный взлом -4
Качественный лед обычно использует сообщения, пересылаемые между программами - например, Watchdog действует на основании данных Trace или система прекращает работу при провале попытки Sever (чтобы предотвратить доступ хакера к информации). Программа Success используется для передачи в систему ложной информации.
Например, Recon сообщила нетраннеру, что Watchdog настроена на запуск Sever, если Trace определит, что сигнал идет не с узла "Альфа". У нетраннера нет нужной для такого случая программы Disguise, и он не хочет использовать умение по умолчанию, поэтому начинает атаку с уничтожения Trace (скорее всего с помощью Corrode). Как только Trace убрана, перед ним возникает проблема - Watchdog, которая ожидает от Trace информации. Декер запускает Success, и она имитирует правильный ответ.
Мастер должен выполнять проверку программы Success каждый раз, когда она должна выдать кому-то ответ. Неудача означает, что это не удалось, и нетраннер знает об этом. При критической неудаче программа не понимает, что ее

раскрыли, и не предупреждает своего владельца... Мастер должен давать бонус программе Success, если нетраннер знает атакуемую систему или уже сталкивался с ней.
Сложность 3, время выполнения 1, стоимость 12,500$.

Skeleton Key
Компьютерный взлом -5 или Программирование -3
Skeleton Key может "открыть" Datalock (проводится состязание умений), обеспечивая доступ к защищенной информации. Skeleton Key использует несколько изощренных (и сложных) криптографических алгоритмов и бывает двух типов. Skeleton Key I по умолчанию имеет уровень умения 10 вместо 12, время выполнения 5, Сложность 2, и стоимость 25,000 $. Максимальный уровень ее умения - 14.
У более сложной Skeleton Key II обычный уровень умения по умолчанию 12, время выполнения 8, Сложность 3, и стоимость 50,000 $. У нее нет максимального уровня умения.

Trace
Использование кибердеки -3
Программа Trace может, достаточно долго двигаясь по электронному следу, оставленному нетраннером, отследить ком-линию, по которой он вышел в сеть. Это может применяться для определения имени и адреса цели (см. поля, стр. 80).
Каждый раз, когда цель прыгает на другой узел, возвращаясь по пути, по которому он вошел в систему, преследователь должен сделать успешную проверку умения Trace, чтобы последовать за ним. Эта проверка производится с пенальти -1 за каждый прыжок разницы между ним и целью (на усмотрение мастера), поскольку трудно преследовать противника, чья кибердека быстрее. Если беглец запускает Misdirection или Codewall, преследователю придется остановиться и сначала справиться с ними (используя Bloodhound и Crumble соответственно).
В случае провала Trace теряет след беглеца, если только он не находится достаточно близко, чтобы его было "видно" в сети (то есть на расстоянии одного прыжка за единицу Сложности машины преследователя).
Если взломщик не отключается от системы и "бежит", сохраняя подключение, то Trace будет наносить ему ущерба, но начнет отслеживать его путь в обратном направлении со скоростью один прыжок в этап. Если она провалит бросок, то сможет немедленно попробовать снова с накапливающимся пенальти -1. Только самая бестолковая Trace не сможет отследить активную линию.
Пример: Мегакорпорация запускает программу Trace 14, чтобы проверить и схватить нетраннера, шпионящего за бухгалтерским компьютером. К сожалению для них, у него очень мощная дека - он делает три прыжка прочь из системы еще до начала работы Trace. Так как он на расстоянии в три прыжка, Trace делает проверку против 11, чтобы повторить его первый прыжок.
Если бы декер после этого остановился, Trace бросала бы против 12 на втором узле и против 13 - на третьем.
Время выполнения 1, Сложность 2, стоимость 20,000$.

Transfer
Компьютерный взлом -6
Эта программа используется для перемещения ценностей (денег или товаров) с одного узла на другой (см. стр. 80). Сама она ничего не может - ей нужно точно сообщить, какие делать прыжки и какие давать пароли (или какие запускать программы), чтобы сделать перевод. Если ее работа по любой причине прервана до завершения (например, прервалась связь или программа наткнулась на неожиданный лед), товар "исчезает" на 1d дней, пока его законные владельцы разбираются с проблемой.
Когда Transfer отработала, мастер делает проверку ее умения. Успех показывает, что она точно следовала инструкциям, а неудача - что что-то пошло не так.
Время выполнения 1 (плюс протяженность ее пути), Сложность 2, стоимость 25,000$.

Webster
Компьютерный взлом -5
Это стандартный ответ на программы Password (см. стр. 93). Она грубо подбирает пароль. Атака проводится как состязание умений между Webster и Password. Webster получает пенальти -5 в защищенной системе и не способен атаковать Datalock.
Если Webster проваливает проверку, хакер может попытаться запустить ее снова с пенальти -3. Некоторые из программ Password поднимают тревогу после первой же неудачной попытки, в то время как другие позволяют неограниченное их число.
Время выполнения 2, Сложность 2, стоимость 5,000$.

ЛЕД

Лед предназначен для защиты. У подобных программ редко есть значение по умолчанию или время выполнения - они или запущены или нет. Защитные программы обычно легальны, хотя использование Black Ice и Misdirection иногда регламентируется.
Самая смертоносная защита - быстрый декер. Чем лучше защищена система, тем вероятней, что в ней задействованы нетраннеры. Для каждой системы мастеру следует решить, задействованы ли там операторы, насколько они хороши, как быстро войдут в сеть по вызову и когда их вызовут.
Кое-какой лед можно использовать для защиты в сетевой битве - отчаявшийся нетраннер может, например, использовать Password, чтобы заблокировать доступ к последней посещенной системе и замедлить преследователя . Если у декера нет нужной программы в слоте, некоторые из них можно запустить по умолчанию.

Alarm
Alarm устанавливают для активизации программы или сигнала (звонка, писка на пульте сисадмина, и т.д.) при попытке несанкционированного доступа к системе. См. также Recon (стр. 91) и Silence (стр. 91).
Программа Alarm запускается (то есть включается) при загрузке системы. Для ее активации нужен один этап. Сложность 2, стоимость 10,000$.

Bailout
Нет значения по умолчанию
Защищает от бесконечных циклов, вызванных Loop (см. стр. 90). Мастер должен устроить провести состязание между программами. Bailout включается после старта системы, Сложность 2, стоимость 15 000 $.

Black Ice
Нет значения по умолчанию
Защитная версия Flatline (стр. 90). Запускается Alarm (стр. 92). Использование Black Ice почти всегда запрещено для частных лиц; его могут использовать только очень влиятельные корпорации. Время выполнения 1, Сложность 4, стоимость 200,000$.

Bluff
Нет значения по умолчанию
Используется для "имитации" льда и представления защиты системы в лучшем виде, чем она есть. Каждая активная программа Bluff может "изобразить" один тип льда. Подробнее см. в описании Recon (стр. 91). Сложность 1, стоимость 1,000$.

Camouflage
Нет значения по умолчанию
Используется, чтобы скрыть линию связи, которая останется невидимой до тех пор, пока кто-то не будет специально искать именно ее (она не видна при общем сканировании сети). Если кто-то пробует найти эту линию, Мастер должен устроить быстрое состязание умений между Camouflage и умением Компьютерного взлома (Computer Hacking) или Использования кибердеки (Cyberdeck Operation) нетраннера. Каждая новая попытка того же декера с той же аппаратурой, получает накопительный штраф в -1. Если он модернизирует свое оборудование или умения, штрафы отменяются.
Сложность 2, стоимость 1,000$ за единицу умения программы. Времени выполнения нет - если Camouflage не будет запущен до появления взломщика, делать это позднее нет смысла.

Codewall
Использование кибердеки -3
Это "стена" сенсорных помех, созданная для временного блокирования проходящего по линии сигнала. Если есть несколько маршрутов из точки А в точку Б, одна Codewall перекроет только один из них.
Codewall разрушается Crumble или распадается сама спустя десять секунд. Время выполнения 2, Сложность 2, стоимость 10,000$.

Datalock
Программирование -4
Datalock по существу представляет собой длинную, сложную, постоянно изменяющуюся версию программы Password. Datalock обычно ставят на отдельные базы данных или программы, а не на систему в целом. Webster не помогает против нее - она может быть снята только с помощью Skeleton Key. У легального пользователя есть ключ; это может быть сообщение, посылаемое его системой или отдельно подключаемый электронный ключ. Код меняется со временем, так что даже "подслушанное" сообщение бесполезно уже через 5 секунд! Время выполнения Datalock составляет 5, но обычно она запускается при старте системы.
По желанию владельца программа может быть встроена в базу данных. В этом случае любая попытка ее уничтожения или даже отключения привилегированным пользователем приведет к уничтожению базы данных!
Сложность 2, стоимость 20,000$.

Disinformation
Нет значения по умолчанию
Используется для подачи ложной информации программе Recon. Мастер должен делать бросок каждый раз, когда Recon (см. стр. 91) провалит попытку обнаружения какого-либо льда. При успехе программа вернет персонажу ложную информацию. У Disinformation нет времени выполнения, она запускается при старте системы. Сложность 2, стоимость 15,000$.

Mask
Нет значения по умолчанию
Используется, чтобы скрыть уровень обороноспособности системы. Mask вычитает 2 из всех попыток исследования системы программой Recon; можно закрыть часть защиты, намеренно оставив другую неприкрытой. За каждое удвоение цены из проверки Recon вычитается еще 1, до максимума в -6 (320,000$). Сложность 2, стоимость 20,000$.

Password
Программирование -2

Это один из простейших способов защиты от несанкционированного доступа. Кроме кражи паролей или применения социотехники (см. стр. 70), для ее нейтрализации может применяться Webster (см. стр. 92) - хотя хорошая программа Password может задать слишком сложные для обычной Webster пароли. Сложность 1, стоимость 100$.
Некоторые из них используют "приглашение", на которое отвечает пользователь, и потому их невозможно прикрыть с помощью программы Mask. Это возможно только когда Password бездействует до получения правильного отзыва.
Обратите внимание, что Password не обязана использовать ввод с клавиатуры. Она может получать данные с любого периферийного устройства или сенсора (см. стр. 53-54).

Regenerate
Нет значения по умолчанию
Regenerate постоянно проверяет целостность всех программ в системе. За один этап она проверяет состояние одной программы. Если она не повреждена, Regenerate переходит к следующей. По умолчанию проверка осуществляется в алфавитном порядке, но сисадмин может произвольно "программировать" Regenerate - например, чтобы она каждый второй цикл проверяла целостность заданной базы данных.
Если программа отсутствует, Regenerate автоматически сообщает об этом. Если она повреждена (например, программой Corrode или неудачной попыткой Silence), мастер делает проверку на умение Regenerate. При успехе она замечает ошибку и принимает меры. Она может восстановить программу из ПЗУ, если это возможно; это занимает один этап для программы Сложности 1, два этапа для программы Сложности 2. Если поврежденная программа находится на диске, Regenerate предлагает оператору запустить ее с независимой (предположительно неповрежденной) резервной копии, и, возможно, выключить на это время систему. Regenerate может также одновременно с началом восстановления активировать другие программы (например, Alarm). Время выполнения 1, Сложность 2, стоимость 30,000$.
Чтобы полностью обезопасить себя от Corrode, нужны две наблюдающие друг за другом программы Regenerate!

Safety Net
Нет значения по умолчанию
Обеспечивает устойчивость работы системы. Каждый раз, когда дается команда, способная привести, например, к перезагрузке системы, она выясняет, есть ли что-то необычное в этом запросе - просматривает внутренний журнал регистрации с целью определить, перезагружается ли обычно система в это время, посылал ли этот пользователь подобный запрос ранее и т.д. Если есть сомнения по поводу легальности запроса, Safety Net отменяет его и посылает соответствующую информацию сисадмину. См. Crash (стр. 89) для получения дополнительной информации.
Safety Net запускается при старте системы. Сложность 2, стоимость 12,000$.

Watchdog
Нет значения по умолчанию
Watchdog постоянно в работе, программа отслеживает и проверяет все подключения к заданному узлу. Некоторые из программ Watchdog просто записывают все подключения в журнал регистрации, другие запускают программы Alarm, Trace или Sever в ответ на любое нелегальное подключение. Watchdog тратит всего этап на запуск другой программы (плюс время ее выполнения).
Сложность 2, стоимость 20,000$.

КАРТА СЕТИ

[рис. стр. 94]

Описание систем
Ниже описан небольшой участок сети. Он может находиться где угодно, но количество прыжков между №106 и KarNet должно соответствовать расстоянию до Берлина.

№101 "Домашний узел" служит для определения расстояния. Это кибердека Сложности 2 с одной ком-линией. Она отключена от сети, когда не используется, так что попытки вторжения бесполезны.

№102 Это GloCom, средних размеров коммерческий компьютерный сервис. GloCom находится под управлением микрофрейма Сложности 4 с этапом продолжительностью 2,000 мс. У GloCom есть несколько гостевых аккаунтов, так что его защита не очень хороша. У него есть четыре стандартных слота с запущенными Password 15, Datalock 14, Regenerate 13 и Safety Net 13.
При каждом подключении запускается программа Password. Datalock используется, чтобы защитить файлы пользователей зашифрованным (см. стр. 63) списком паролей. Любой, получив доступ к этой базе данных, сможет, вероятно, расшифровать их и получить список всех аккаунтов. Также в системе есть запущенная с диска Alarm 12. Если Regenerate обнаруживает повреждение системы, она активирует ее. Alarm просто подает звуковой сигнал на главный системный пульт, за которым круглосуточно дежурит оператор.

№103 Это DataLok, малый банк данных. Он запущен на модернизированном мейнфрейме Сложности 5. У него 10 слотов вместо обычных 5, а быстродействие увеличено на 25%, что дает продолжительность этапа в 750 миллисекунд. Подключены программы: Alarm 13, Bailout 12, Camouflage 13, Datalock 18, Mask 13, Password 17, Regenerate 13, Sever 13, Trace 14 и Watchdog 15.
Структура защиты: Все входящие линии прикрыты с помощью Camouflage - их могут обнаружить пользователи DataLock, но при обычном просмотре обнаружить их нельзя. Чтобы скрыть защиту, в системе также запущена Mask. Watchdog отслеживает все подключения и попытки входа в систему. Если за первые 10 секунд после подключения не

был осуществлен успешный вход в систему, она запускает Sever. Если программа Sever не сработала, она запускает Alarm, которая предупреждает оператора и запускает Trace.
Password предупреждает Watchdog о каждом успешном входе в систему. Если Password уничтожена программой Corrode или иным способом, она перестанет посылать Watchdog сообщения и та запустит Sever.
Все базы данных защищены Datalock и хранятся в зашифрованном виде (см. стр. 63). Если Regenerate обнаружит повреждение Datalock, она немедленно запускает Sever и Alarm. Если Sever не сработает, она активирует Trace и начинает запуск с диска (не с ПЗУ-карты, так что время выполнения 4) программ Codewall перед взломщиком. Она будет продолжать запуск Codewall и Sever каждый этап, пока это подключение не будет прервано (или пока с Watchdog чего-нибудь не случиться...). Если Regenerate обнаружит повреждение Watchdog, она немедленно начнет запуск тех же Codewall и Sever, но остановится только по приказу оператора.
Кроме пароля на входе, каждый участок данных опять же защищен программой Password, которую тоже нужно пройти. Информация, которая хранится в этой системе, остается на усмотрение мастера, но она должна быть ценной.

№104 Это общественная система BBS, принадлежащая Обществу Творческой Анархии. У нее одна входная линия (который занята при результате 13 или меньше броска 3d), и нет защиты, кроме обычной Password 12. Помимо участия в многочисленных дискуссиях, многие нетраннеры заходят сюда для проверки почты. Конечно, никто в своем уме не оставит тут ничего ценного, но здесь удобно договариваться о дальнейших встречах. Продолжительность этапа 8,000 мс

№105 Это миникомп, обеспечивающий деятельность Cap, Inc (компания по производству колпачков для тюбиков зубной пасты). В компании работает 23 человека, ее прошлогодний доход составил 1.8 миллиона $. Продолжительность этапа системы составляет 4,000 мс, подключены программы Password 15, Alarm 12 и Bluff 12 (имитирующая Black Ice).
После трех неудачных попыток пройти Password или одной попытки подавить Bluff, имитирующую Black Ice (все легальные пользователи не обращают на нее внимания...) запускается Alarm. Она подает сигнал на пульт оператора, но это имеет значение только в рабочее время.

KarNet
Эта часть сети - принадлежащая KarNet мини-сеть. №107 "виден" только из №106, да и то если до Берлина не слишком далеко. Остальная часть сети видна только из №107 при наличии правильного пароля для одной из ком-линий удаленного доступа.
Кроме шлюза №106, система KarNet не поддерживает подключения извне системы. Есть одно исключение: см. №109.

№106 Это сетевой шлюз к KarNet (внутренняя сеть ведущего немецкого автомобилестроителя). Шлюз поддерживает до 8 пользователей одновременно при запущенной Password 16.

№107 Эта линия связи позволяет инженерам и дистрибьюторам KarNet использовать компьютеры главного офиса и гарантирует безопасность сделки. Замок запущен на микрофрейме Сложности 4 с увеличенным на 25% быстродействием (этап длится 1,500 миллисекунд). Кроме того, у него 8 слотов вместо обычных 4.
Подключены программы Password 18, Trace 15, Bloodhound 14, Disinformation 16, Watchdog 15, Snare 13, Regenerate 13 и Alarm 14.
Задействована двухуровневая система паролей. Первая программа Password активируется при подключении. Если ее успешно пройти (применив Webster или легальный пароль), пользователя встретит "сисоп-в-коробке" (см. стр. 80), который начнет задавать вопросы из базы данных (защищенной Datalock 13 с диска). Для подключения с узла №107 к внутренней сети нужно пройти еще одну программу Password.
Watchdog отслеживает все подключения; Disinformation постоянно активна. Если попытка пройти программу Password не удалась (неудача при использовании Webster или при проверке на Компьютерный взлом), она одновременно запускает Snare и Alarm, которая подает сигнал на главный пульт (круглосуточное дежурство). После запуска Snare Watchdog активирует Trace (использующую Bloodhound, если нужно).
Regenerate также запускает Snare и Alarm при выявлении любой попытки повреждения программ.

№108 Эта система обслуживает более чем пятитысячный рабочий персонал Karwerks. Сисадмины полагаются на защиту Замка (№107), поэтому подключены только программы Password 14 и Regenerate 12. Продолжительность этапа системы - 2,000 мс.
Система занимается зарплатой и отпусками служащих - она не делает проверок, но высылает информацию об отработанных часах в систему №111, который занимается бухгалтерией. Она также ведет личные дела персонала - заявления, результаты собеседования, занимаемые должности, изменения в зарплате, и т.д.

№109 Это частный спутниковый канал связи KarNet. Он обеспечивает быстрый доступ к другим системам KarNet во всем мире. Прежде всего его использует отдел исследований и разработок системы №110. Здесь запущены Trace 12 и Alarm 13. Все подключения отрабатываются Trace. Любое подключение, сделанное не из №110, проверяется по небольшой базе данных привилегированных пользователей на других машинах. Если аккаунт не соответствует привилегированному, Alarm подает сигнал на системный пульт. Тот факт, что эта система принимает входящие звонки, делает ее огромным черным ходом в систему KarNet.

№110 Все вычисления отдела исследований и разработок Karwerks обрабатываются этим мейнфреймом. Продолжительность его этапа - 1,000 миллисекунд. Как и №108, он не слишком полагается на собственную защиту - сисадмины больше доверяют Замку.

В этой системе запущены: Password 13, две программы Regenerate 13 (наблюдающие за системой и друг за другом) и Alarm 14. Кроме того, все данные защищены Datalock 14, находящейся на диске. Если любая из программ Regenerate обнаруживает повреждение системы, Alarm подает сигнал на системный пульт.

№111 Это главный финансовый компьютер Karwerks. Он занимается счетами, подлежащими оплате, счетами-фактурами, зарплатой и всем, что связано с бухгалтерией. Внешние подключения происходят не часто, поэтому здесь только две ком-линии. Продолжительность этапа системы составляет 2,000 мс.
Защита основана на обнаружении нелегальных пользователей и вызове операторов. Здесь запущены Password 14, Trace 13, Bloodhound 13 и Alarm 13. Каждое подключение автоматически отслеживается - если это не привилегированный пользователь с машины №108, запускается Alarm.

ПРИМЕР НЕТРАННИНГА

Нашего отважного хакера Злого Стиви, наняли для взлома KarNet с целью узнать имя руководителя исследовательских работ по проекту Boxon 2000.
Он экипирован кибердекой Макси-3 (Сложность 3, ИБ 4, продолжительность этапа 1,000 мс, нет дополнительных слотов) с Promote 14, Recon 15, Corrode 13 и Silence 13. Нужные умения - Компьютерный взлом 14, Программирование 13 и Использование кибердеки 13. Посредник, нанявший Стиви, сказал ему номер узла (№106) шлюза KarNet и предупредил его о Замке с другой стороны. Дальше него никто пока не добирался!
Стиви подключается к узлу №101 и осматривается. Он видит №102, №104, и №105. (Так как не ищет его специально, №103 (Datalok) невидим благодаря прикрытию Camouflage). Он также видит шлюз №106 на расстоянии одного прыжка, и посылает туда Recon для его изучения. Мастер скрытно бросает на Recon 15 для системного льда (только Password) - успешно. Он сообщает игроку, что тот увидел только Password. Поскольку программ Watchdog нет, Disguise бесполезна (она не помогает против Password). Он может или использовать Webster по умолчанию, или применить Corrode. Он выбирает последнее.
Проводится быстрое состязание между мастером (Password 16) и Стиви (Corrode 13). Мастер выбрасывает 14, успех на 2; Стиви выбрасывает 10, успех на 3. Программа Password разрушена, система осталась без защиты, и Стиви входит.
Поскольку эта система - просто канал передачи данных, Стиви нечего не остается, кроме как пойти дальше. Он запускает Promote, чтобы получить права получше, но здесь это невозможно. Эта точка слишком далека от Берлина (вероятно), чтобы он увидел хоть что-то, кроме ограниченной и невыразительной части уходящего вдаль киберпространства. По мере приближения к №107 (Замок), он начнет различать детали. Он высылает Recon, которая может обнаружить Password, Watchdog, Regenerate, Disinformation и Alarm. Recon обнаруживает все, кроме Disinformation. Тогда мастер успешно выполняет проверку Disinformation 16, и решает, что Recon сообщила Стиви о наличии впереди Black Ice. Стиви прыгает ближе и мастер начинает отслеживать время, отметив, что Regenerate проверяет программы по одной в этап в следующем порядке: Watchdog, Bloodhound, Disinformation, Password, Trace, Snare и Alarm. Сейчас она осматривает Trace.
Здесь мастер должен сообщить Стиви, что его этап короче, чем у Замка - но не сообщать, на сколько именно!

0.0 секунд: Стиви сталкивается с первой программой Password, и пытается взломать ее, запустив Webster по умолчанию. Он выбрасывает 7 - успешно. Regenerate начинает осматривать Trace.
1.0 секунд: "Сисоп-в-коробке" начинает задавать Стиви вопросы. Не мудрствуя лукаво, тот запускает против него Corrode, одновременно посылая на Alarm программу Silence (проверка Использования кибердеки -3 за два действия в одном этапе. У него получается). Corrode выигрывает быстрое состязание с СВК и уничтожает его. Однако против Alarm программа неэффективна, и Regenerate может скоро заметить повреждения в системе!
1.5 секунд: Regenerate заканчивает проверку Trace и принимается за Snare.
2.0 секунд: Стиви понимает, что скорее всего, скоро начнуться проблемы. Он запускает дополнительную программу Promote (Программирование -2 минус Сложность системы - эффективное умение 7). Это займет 2 этапа.
3.0 секунд: Продолжается запуск Promote. Regenerate закончила с Snare и начала проверку Trace.
4.0 секунд: Стиви выбрасывает 9 на Promote - неудача. Ругаясь, он снова запускает Silence, но она не срабатывает.
4.5 секунд: Regenerate выполняет проверку и обнаруживает, что на Alarm нападали. Она запускает Snare и активирует Alarm. После этого, согласно собственным настройкам, начинает запускать копию Alarm. Стиви видит начало запуска Snare.
5.0 секунд: Snare не сработает раньше 6.0 секунд. Стиви решает, что осторожность - это лучшая доблесть и отключается, оставаясь ошеломленным на 3 секунды.
6.0 секунд: Snare срабатывает в пустой ячейке матрицы, которую Стиви покинул мгновение назад. Оператор отвечает на Alarm, но кроме уничтоженной программы СВК, не находит ничего необычного.

Оригинал:
GURPS Cyberpunk
Chapter Four: Netrunning. Стр. 61-95

Перевод (с) Sergeant
Редактура (с) Junior
http://www.utkgurps.narod.ru/